IN THE DISTRICT COURT OF THE UNITED STATES
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	Judge Gaughan
	)	Cleveland, Ohio
vs.	)	
	)	Number 1:16CR224
BOGDAN NICOLESCU,	)	
RADU MICLAUS,	)	
	)	
Defendants.		

- - - - -

TRANSCRIPT OF PROCEEDINGS HAD BEFORE

THE HONORABLE PATRICIA ANNE GAUGHAN

JUDGE OF SAID COURT,

ON WEDNESDAY, MARCH 27, 2019

Volume 3

- - - - -

Official Court Reporter: Shirle M. Perkins, RDR, CRR
U.S. District Court
801 West Superior, #7-189
Cleveland, OH 44113-1829
(216) 357-7106

Proceedings recorded by mechanical stenography; transcript produced by computer-aided transcription.

APPEARANCES:

For the Government:

DUNCAN T. BROWN,
BRIAN MCDONOUGH,
Assistant U.S. Attorneys
801 West Superior Avenue
Cleveland, OH 44113
(216) 622-3600

BRIAN LEVINE,
U.S. Department of Justice -
Criminal Division
Ste. 600
1301 New York Avenue
Washington, DC 20530
(202) 616-5227

For Bogdan Nicolescu:

MICHAEL GOLDBERG, ESQ.,
Goldberg & O'Shea
Suite 450
323 Lake Place
Cleveland, OH 44113
(216) 696-4514

For Radu Miclaus:

MICHAEL J. O'SHEA, ESQ.,
Lipson O'Shea
110 Hoyt Block Bldg.
700 West St. Clair Avenue
Cleveland, OH 44113
(216) 241-0011

WEDNESDAY SESSION, MARCH 27, 2019, AT 8:37 A.M.

THE COURT: Counsel, may I see you at side bar.

(The following proceedings were held at side bar:)

09:05:15 THE COURT: Mr. Brown handed the Court an ex parte motion under seal. Am I correct that it has not been filed as of yet?

MR. BROWN: That's correct.

THE COURT: All right. It's a Government's in
09:05:40 camera motion for ex parte determination of Giglio
disclosure.

I think -- I'm not certain -- I believe that this really has to be done in two steps. I think the Government first has to file a motion requesting that they be permitted
09:07:19 to file the in camera motion. I'm just going to orally
indicate that you can.

MR. BROWN: Thank you.

THE COURT: And I now have before me the motion that sets forth the information.

09:07:40 Upon review of the information, I do not find that this matter needs to be disclosed.

You do need, however -- you have to file it under seal ex parte so it can be preserved for appellate purposes.

MR. BROWN: I will have my assistant do that
09:08:04 this morning. Thank you very much, your Honor.

THE COURT: Thank you.

MR. GOLDBERG: I was just going to say I'm going to --

THE COURT: Off, Shirle.

09:08:20 (Discussion held off the record.)

(Proceedings held in the presence of the jury:)

THE COURT: Good morning, ladies and gentlemen.

THE JURY: Good morning.

09:14:27 THE COURT: Mr. Levine, you may continue.

MR. LEVINE: Thank you, your Honor.

THE COURT: And, ladies and gentlemen, by the way, if you see James here walking around, he's helping us with our technology. And I have given him permission to 09:14:40 have free reign of the courtroom while we're in, while we're in session.

So again, James, you feel free to do whatever you have to do, even while we're in session.

You may continue.

09:14:56 DIRECT EXAMINATION OF LIAM OMURCHU

BY MR. LEVINE:

Q. Okay.

Mr. Omurchu, just for the record, did we have any conversations at all since you left the stand yesterday?

09:15:02 **A.** No.

Q. Okay.

I'm just going to remind you to let me finish asking
my question just so the Court Reporter can clearly get my
question and your answer. Is that okay?

09:15:12 **A.** Yes, that's fine.

Q. Thank you so much. All right.

So yesterday we were talking about the Bayrob Trojan.
You recall that?

A. Yes.

09:15:19 **Q.** And do you know where the Bayrob Trojan got its name?

A. Yes, I named it.

Q. You named it?

A. That's correct.

Q. Okay.

09:15:28 Why did you name it the Bayrob Trojan?

A. Well, because when I investigated it, it was trying to
rob the people who were using eBay. So I took those two
words and put them together and I created the word Bayrob,
and that's how I named it.

09:15:44 **Q.** And is that -- is it common for security researchers
who identify malware to name that malware?

A. Yes, it is.

Q. Okay. All right.

So yesterday, we looked at some examples of spam
09:16:00 e-mails that contained the virus and files, do you recall

that?

A. Yes, I do.

Q. And can you remind us, where did you find those spam e-mails that had the virus attached to them?

09:16:12 **A.** Those e-mails -- my infected machine with the Bayrob virus on it was sent instructions from the command control server to send those e-mails with the Bayrob Trojan attached to them.

Q. Okay.

09:16:28 Including the one that said you have AIDS and here are the test results?

A. Yes, that's correct.

Q. All right.

Now, we were talking about who the Bayrob Group would 09:16:40 send this spam to. And so generally, how would they -- how would they get e-mail addresses to spam -- to send the spam e-mails to?

A. So there's lots of different ways to get e-mail addresses, and they used multiple different schemes to get 09:16:55 e-mail addresses.

And one of them was to take e-mail addresses from infected computers, from the address book of infected computers, and then another way was to search on the web for e-mail addresses and on web pages that they could then use 09:17:12 to send people e-mails.

Q. All right.

So I'd like to bring up what's been previously marked as Government's Exhibit 1422, which is a two-page exhibit. And this can be published to the jury. I don't see it yet. 09:17:45 Thank you so much, James.

THE COURT: There we go.

MR. LEVINE: Okay, great.

THE COURT: Folks, you see it on the screen?

THE JURY: Yes.

09:17:52 THE COURT: All right.

MR. LEVINE: Excellent.

Q. Okay.

So this is a two-page exhibit. Can you tell us, first of all, what is -- well, make sure you see both pages. If 09:18:03 you look at the first page here and if we could see the second page. Okay.

So let's go back -- well, let's go back to the first page. And if you could tell me what -- what is this we're looking at here?

09:18:24 **A.** So you're looking at a web page for the -- this is a screenshot I took of a Florida Bar website. And the second part of this is a log that was sent from my infected computer to the command and control server, recording the information taken from the Florida Bar website.

09:18:46 **Q.** Okay.

So first of all, let's break this down a bit. You said screenshot?

A. Yeah.

Q. Can you tell us what's a screenshot?

09:18:53 **A.** So I visited this web page on my computer and then I took a -- sent, took a picture of it and saved that picture.

Q. Okay.

So a screenshot is just a picture of something that you see on the screen?

09:19:04 **A.** Yes.

Q. And when you take a picture of something on the screen with the screenshot, is it an exact picture of what you see on the screen?

A. Yes, it is, yes.

09:19:12 **Q.** Okay.

And so what -- what was your computer being instructed to do by that code we see on the second page there?

A. Well, the code we see on the second page is actually the results of what my computer, infected computer was asked to do. 09:19:28 So my infected computer was asked to visit the Florida Bar website and then to look at the text on the Florida Bar website and try to find contact information on that page, and then extract that contact information and send that to the command and control server.

09:19:49 **Q.** Okay.

So just real quickly if we can look at the first page. What is the Florida Bar website?

A. So the Florida Bar website shows -- well, at this page shows member information, contact information for lawyers in the Florida Bar. 09:20:05

Q. Okay.

So it's a web page that, among other things, has contact information for lawyers in Florida?

A. Yes, exactly.

09:20:16 **Q.** And your computer was instructed to go out and pull that contact information?

A. That's correct.

Q. And what -- where was it instructed to send that contact information?

09:20:28 **A.** It was instructed to send it back to the command and control server.

Q. Is there a name for the process of going out onto the web and pulling down information like that from publicly available websites?

09:20:41 **A.** Yes, it's called web scraping.

Q. Okay. And why is it called web scraping?

A. Well, you're trying to, sort of similar to, you know, scraping paint or something like that, you're trying to look through the content that's there and take out a little piece that you're interested in and do something with that. So -- 09:20:57

yeah, that's why it's called web scraping.

Q. Okay.

And based on your investigation, what other websites did the Bayrob Group scrape to get e-mail addresses for spamming? 09:21:15

A. They scraped lots of different websites that -- particularly, the Yellow Pages, and they would search for hotels on the Yellow Pages website and then when they got the results, they would go through the page to try and find 09:21:30 an e-mail address to contact that hotel or anything else that they searched for, and they did that in multiple countries in the U.S. and Germany and Spain and France, different Yellow Pages websites, and they also searched travel websites, Trip Advisor, which is a website for 09:21:51 helping you travel.

Yeah, lots of -- lots of different websites. Any website that, lots of different websites that had e-mail addresses on the page where they could automatically get that e-mail address and record it.

09:22:06 **Q.** Okay.

So I just want to make sure I understand one thing you said there. You referred to Yellow Pages?

A. Uh-huh.

Q. Is that related to the big yellow book that gets 09:22:17 dropped in my driveway every --

A. Yes, it's the online version of a -- of that book. So it's a directory of information, telephone numbers, contact information. It's just available online instead of in the -- in the book and --

09:22:31 **Q.** In the online version, they have e-mail addresses as well?

A. Yes, they have e-mail addresses as well. And in the online version, not just telephone numbers.

Q. So the Bayrob Group scraped information from the 09:22:45 Internet for e-mail addresses to send to spam that we looked at earlier?

A. Yes, that's correct.

Q. All right.

I'd like to show you what's been previously marked as 09:22:55 Government's Exhibit 1423. And we can publish this to the jury. And maybe zoom in on the bottom text here. Okay.

Can you tell us what we're looking at here at Exhibit 1423, which I'll represent is a three-page exhibit?

A. This is a log that was sent from my computer to the 09:23:28 command and control server, my infected computer to the command and control server, showing activity that happened on my computer.

Q. Okay. And what activity is it showing here?

A. It's showing messages being sent via Facebook Chat.

09:23:46 **Q.** Okay. So your computer was instructed to send messages via Facebook Chat?

A. Yes, that's right.

So my infected computer received a command from the command and control server and asking my machine to send 09:24:02 messages on Facebook Chat.

Q. First of all, I know some people might be familiar with this but what is Facebook?

A. Facebook is a social media website, an application where you can connect with friends and family and share 09:24:22 information, photos and messages.

Q. Okay. So what is Facebook Chat then?

A. Facebook Chat allows you to have direct conversation with one of your contacts, where you can put in their name and then you can have it -- a little chat window and you can 09:24:41 type a message and they can respond.

So you can have a conversation in real time with your -- with your friends.

Q. Is that similar to texting?

A. Yeah, it's -- yeah, it's pretty similar to texting, 09:24:53 yeah.

Q. If we can look at the second page of this exhibit, please. Thank you so much, Sue. All right.

And this is -- the second page, please. Yeah, we can show the whole thing for right now and maybe we will zoom in 09:25:13 on a portion in a little bit. But, can you tell us what this is, Mr. Omurchu?

A. So this is template for spam messages that my computer was asked to send.

Q. And were these -- the ones that they were asking your
09:25:32 computer or instructing your computer to send over Facebook Chat?

A. I believe these are being sent via e-mail and not over a Facebook Chat. And on the previous page the message was being sent over Facebook Chat.

09:25:57 **Q.** Okay.

So this second page are messages that your computer was instructed to send over e-mail is your recollection.

A. Yes, that's my recollection.

Q. Okay.

09:26:07 Can you tell us what this is because it looks real -- I mean I see the words here but looks relatively unreadable.

A. Yes.

So in order to send spam messages, those e-mail messages are going to be blocked by companies like Symantec.
09:26:24 And so what the virus writers do or spammers do is try to vary the text in the e-mail every time. So instead of saying in this case, there's a big reward for catching -- so this -- this template is about Paul Walker. So Paul Walker, an actor in the Fast and the Furious, and he had been in a
09:26:49 car crash and had passed away in the car crash. And after

that incident, my computer was asked to send spam that was pretending to be from the police asking for information in re, in regards to that crash. And they had an attachment to that e-mail, which was actually the Bayrob virus.

09:27:08 So if you felt you were getting information about the crash, and you went to read that information, you would actually get the Bayrob virus instead and your computer would get infected.

And what this here is doing is it is telling my 09:27:22 computer that there are lots of different ways for my computer to send that e-mail about Paul Walker. So at the beginning, you can see that -- well, let's look at the top line. You can see reward, the word reward and then there's a caret symbol and compensation and caret symbol and 09:27:43 reimbursement and a caret symbol and pay back on top line. And what that tells my computer is when I compose that e-mail to send, I can choose any one of those words to put in. I only choose one. So I can say the e-mail might read, "There is a big reward," or, "There is a big compensation," 09:28:00 or, "There's a big reimbursement," or, "There's a big pay back."

And in that way, they vary the text in the spam e-mail every time. So every time my computer sends an e-mail, it will have a different combination of words in there, and 09:28:14 that makes it difficult for a security company to block that e-mail because it looks different every time. And so this is a template that my computer receives and it's -- it's -- I also see instructions to construct this e-mail and send it out multiple times and choosing different permeations of these words. 09:28:37

Q. And just to be clear, what actually makes the selection of which of all these different words to fill in the blank? Do you personally do that?

A. No, I receive instructions. I receive a program onto 09:28:53 the infected computer. The virus is selecting which combination to choose every time it sends an e-mail so that it chooses a unique combination every time, and every e-mail looks slightly different from the last one.

Q. Okay.

09:29:08 And when you say that you receive this, is it something that the user of an infected computer would normally be aware of?

A. No, this all happens hidden. So there's no visible sign that your computer is infected or that this is 09:29:26 happening in the background.

Q. Okay. And how are you able to see that it was happening?

A. Because I monitored my computer with security tools to be able to understand what my computer was doing, not just 09:29:37 what is visible on my computer but what's actually happening underneath. And also I was recording the instructions sent from the command and control server. And this is some of the instructions that I received.

Q. Okay.

09:29:49 And that was using some of the tools that we discussed yesterday?

A. Yes, that's correct.

Q. I think you said that the Bayrob Group would also send their spam to the contacts of victims whose computers were already infected? 09:30:14

A. Yes, that's correct.

Q. So, for example, if my computer was infected with the Bayrob Malware, could the Bayrob Group make my computer send out malicious spam to my relatives and everyone in my e-mail address book? 09:30:30

A. Yes, they could.

Q. And what would happen if a person clicked on one of the attachments to the spam e-mails we looked at or the Facebook message links?

09:30:40 **A.** With the Facebook message links, they would get infected with the Bayrob Trojan, Bayrob Malware.

Q. If they were sending out my contact list, would it appear to my relatives, or whoever else was getting it, that the e-mail was coming from me?

09:30:58 **A.** Yes. For Facebook Messenger chats, the chat would appear to come from your contact. So it would look very legitimate.

Q. Okay.

So is it fair to say that in some instances, it would 09:31:17 look as though it were coming from the victims' contact -- from the victim himself -- him or herself?

A. Yes.

Q. Some instances would look like it was coming from a third party?

09:31:26 **A.** Yes, that's correct.

Q. Okay.

So now I want to learn a little more about the Bayrob Malware. Was there just one Bayrob Trojan or were there many versions of the Bayrob Malware?

09:31:41 **A.** It was many versions.

Q. Okay.

And how many distinct versions of the malware did you identify?

A. About -- about 70. I think the exact number was 73, 09:31:56 but it was around 70 mini versions.

Q. So it's clear for the record, you're saying 7, 0, 70?

A. Yes, seven zero.

Q. And at a general level, what do we see happening over time in these 70 or 73 versions of the Bayrob Trojan?

09:32:15 **A.** Generally, the Trojan had new features added to it.

It got more sophisticated and it became more protected, and also it changed to avoid detection by security companies, such as Symantec.

Q. Such as your security company?

09:32:33 **A.** Yes.

Q. Okay.

And did each of the 70 or 73 versions of the Bayrob Malware also have variations among the versions?

A. Yes.

09:32:45 So while there was 70, around 70 versions of the core virus, what the -- what the attackers do is they create multiple versions of each, and it create multiple instances of each version.

So for Version 1, for example, if they sent Version 1, 09:33:11 just that one version to thousands of computers, that would get blocked very easily by antivirus, and we would see it. We would understand what it was, know what it looked like and be able to block it.

So to avoid getting blocked, what they do, they create 09:33:28 multiple different variations of that virus. So the same thing underneath but it's wrapped differently or looks slightly different and it changes all the time, so that it's more difficult for antivirus to block it. And for every version, the 70 different versions of Bayrob, they created 09:33:49 thousands or tens of thousands of variants and over those versions to make it more difficult for antivirus detection.

Q. I want to make sure I understand this.

Each one of the 70 or 73 versions had thousands or tens of thousands of variants?

09:34:06 **A.** Yes.

Q. How could a human make tens of thousands of variants times 70? That's like, you know, 70,000 or 700,000, I can't do the math, but that's a lot of variants. How could a human do that?

09:34:21 **A.** They didn't do it manually. They wrote a program to do it so they had a program that would morph the virus very frequently, and they would create, you know, tens of thousands at a time with a program. So they didn't have to manually create them themselves.

09:34:38 **Q.** Can you give us an example of the type of change they would make within like 10,000 variations? Couldn't be a big change. What kind of change would they make for the 10,000 variations of say Version 20?

A. Well, they would -- they would, for example they could 09:34:59 encrypt it, and in which case, they essentially use a key to -- to make each one look different, and they use a different key so that every version looks different. You need a different key to be able to get inside it.

Q. Okay. So these were subtle changes then?

09:35:21 **A.** Sometimes they were subtle. Sometimes they were not but yes, yes, generally described as subtle changes, yes.

Q. To be clear, I'm talking about not the 70 different main versions but the 10,000 variations of each of the 70 main versions?

09:35:36 **A.** Yes, yes.

Q. Those were subtle changes?

A. Yes.

Q. Okay.

And is that -- was that an effective way to prevent 09:35:46 antivirus from identifying the malware?

A. Yes, yes, it was.

Q. Okay. All right.

I'd like to show you what's been previously marked as Government's Exhibit 1424. And we can show it to the jury 09:36:01 as well. If we could zoom in on the top part. Okay. You mentioned something called a hex editor in the beginning of the testimony.

A. Yes.

Q. Is this a screenshot of a hex editor?

09:36:26 **A.** Yes, it is.

Q. Can you tell us what -- what we're seeing there?

A. Sure.

So the very left-hand side, there's a column of numbers with eight digits starting with 004. So that is the 09:36:41 address for the date that is on the right-hand side.

Q. And let me stop you for a second. Step back for a minute.

A. Okay.

Q. Is this an announcement of a particular file?

09:36:51 **A.** Yes, this is an analysis of a Bayrob Trojan.

Q. So we are looking at part of the Bayrob Trojan right here?

A. Yes, you are.

Q. All right.

09:36:59 So now that we know that, let's step back and say what is that column on the left there?

A. So the column on the left is the address and it's like an index into the file, and it tells you where in the file you're looking at, at this particular time.

09:37:15 **Q.** Okay.

So it's like an index or a line number for --

A. Yes, a line number.

Q. For malware?

A. Yes.

09:37:21 **Q.** What's that big thing, big column in the middle where there's red in it?

A. Yes. The big column in the middle is the contents of the file, shown as hex, hex decimal.

Q. Remind us what hex decimal is?

09:37:34 **A.** It's just a way of showing the content in a way that is more readable.

Q. More readable to who?

A. More readable to an engineer or a --

Q. You can read that in the middle?

09:37:47 **A.** Yes, yes.

Q. Okay.

If you -- can the computer read that in the middle?

A. Yes.

Q. All right.

09:37:57 And then what are you seeing on the -- on the right column there?

A. On the right-hand side is the interpretation of what is shown in the middle column, so if -- in the middle column, there may be numbers that are code; in which case, 09:38:18 you can't read them in English but there may be numbers that are -- that represent numbers and letters. And if they are numbers and letters, then on the right-hand side column, it will show you the English translation of the -- and numbers that are in center column.

09:38:35 **Q.** Okay.

So is the highlighted portion to the right where it's has letters and they look like things I can read, is that the same highlighted portion that we're seeing in the middle column?

09:38:48 **A.** Yes.

Q. Okay.

And what -- what does that say there that -- that you've highlighted on this first page?

A. So on the right-hand side is the English version of 09:39:00 the numbers, and what we see there, there's a couple different things there, but the first part is Adrian Cupalume, and it's the name of a -- the name of a Romanian singer. And after that, there's another word I believe is also the name of another Romanian singer, and then after 09:39:24 that, the final piece is, there's an eight-letter word there at the end, pitskey with a colon at the end, and there's some rude words here. I'm allowed to say what they are?

Q. Yeah, you can -- yes. You can see?

A. So this last piece here pizda is the Romanian word for 09:39:52 pussy. And this word here is a marker in the virus to show where the encrypted data is to be found.

Q. Okay.

So and we're going to look at the actual certified translation at the end of this document. Let's go on to the 09:40:14 second page. And if we could zoom in on the first -- the part where there's the highlighting which is kind of the middle there. Okay.

And this is -- what is this page? Is this another portion of the Bayrob Malware?

09:40:36 **A.** Yes, another portion of the Bayrob Malware.

Q. And what were you highlighting here?

A. So I'm highlighting here the websites that the virus was asked to connect to, to receive instructions. So these websites, you see here you'll see there's dot com, some 09:40:51 words at the end, there's a dot com. Those are the websites that -- where the command and control server was, and this is a list of the places where the Bayrob virus should connect out to try and receive commands.

Q. So if I have an infected machine, why would the 09:41:12 computer reach out to websites that are listed there?

A. So this is the list of places where they can receive -- they can be controlled from.

Q. Okay.

So my computer knows to reach out to those websites 09:41:27 and the instructions will somehow be on those websites?

A. Yes, exactly.

Q. What is the one you have highlighted there?

A. So the one I have highlight is ulanesatula.com.

Q. Do you know what that means?

09:41:41 **A.** I do.

Q. What does it mean?

A. It means "insatiable dick."

Q. Okay. In Romanian?

A. In Romanian.

09:41:47 **Q.** All right.

If you could scroll to the next page, please, or zoom in on the highlighted portion. Okay.

And is this also a -- we're looking at a piece of the Bayrob Malware?

09:42:10 **A.** Yes, that's correct.

Q. And what do you have highlighted there?

A. So this is the name of the file that will be created on your computer. So the Bayrob will copy itself to your computer and it will create a file name that is different 09:42:30 every time, different versions, and this is the file name that should be used in this case as to store the Bayrob Trojan on your computer.

Q. And do you know what this file name means?

A. Again, it's something rude in Romanian. I believe 09:42:46 it's "suck the dick," something like that.

Q. Okay.

Let's look at the next page, and if we could zoom in on the same way. Thank you -- thank you so much. Okay. And what -- is this also part of the Bayrob Trojan that 09:43:06 we're looking at?

A. Yes, this is part of the trojan.

Q. Okay. And what have you highlighted here?

A. Again, I've highlighted the websites that the trojan was going to connect out to, to receive instructions. And 09:43:17 these are two more Romanian language websites.

Q. Okay.

And do you know what either of those mean?

A. I believe the first one means spring, winter, maybe, something like that in Romanian. And the second one, again 09:43:39 it's something -- I believe it's something rude. I don't recall exactly.

Q. All right. We'll look at the translation momentarily. Can we scroll through the next page? Okay.

Is this another piece of the Bayrob Trojan we're 09:44:03 looking at, code?

A. Yes, that's correct.

Q. Okay. What does the highlighted portion mean here?

A. So the highlighted portion is when the -- it's -- well, it's a comment. There's a comment in there, which is, 09:44:19 "Sue give websets," which means suck websets, and that's if something went wrong when the virus was running, this is the message that would be sent back to the authors so they can understand something went wrong. But before that, there's a text highlighted which is, "Fool's message," and these are 09:44:39 the parts here, fool's real name, fool's address, things like that. And this is where they would collect infected, from an infected computer would collect a victim information. And they were storing it as the fool's name and the fool's real name and fool's message, and basically 09:44:59 calling the victim fools here.

Q. Can you point to where you're seeing this as a fool's information on the screen? I think you can move that red pointer over.

A. Yeah, sure.

09:45:09 So up here is the fool's message, and then that -- further down is, "Fool's real name," and, "Fool's address."

So when the victim would enter their information into the website, it would be stolen by the virus and sent to the attackers, and this was a place holder for that information. 09:45:38 So when they stole the victim's information they were using. They were describing the victims as fools.

Q. They were storing the victim's real name as, "Fool's real name"?

A. Yes.

09:45:49 **Q.** And the victim's address as, "Fool's address"?

A. Yes, that's correct.

Q. All right.

Can we move to the next page? And the next page, please. And let's just see the -- we'll take a quick look 09:46:03 at the Romanian certified translations here. You say these were names of people?

A. Yes, names of Romanian singers.

Q. Okay. And the last word there is as it was in the original, pizdkey?

09:46:20 **A.** Yes. So that -- that word was originally data key.

So that's the originally in the previous version it was called data key, but Symantec used that to detect the virus. So they had to change it. So when they changed it, they changed it from data key to pizdkey, pussy key instead of 09:46:43 data key.

Q. And is that an example of what you were referring to as a small variation for antivirus?

A. Yes, exactly.

Q. Okay.

09:46:53 Can we scroll to the next page? And zoom in on the translation part. Okay. So that's the -- is this the Romanian translation for that website?

A. Yes, correct.

Q. Okay.

09:47:11 Is that consistent with what you understood it to mean?

A. Yes, it is.

Q. All right. Let's look at the next page.

And this is the translation for the name of a dot EXE 09:47:29 file; is that right?

A. Yes, that's correct.

Q. What is a dot EXE file?

A. It's a file that can run on your computer.

Q. Okay. What does EXE stand for?

09:47:39 **A.** EXE stands for executable. So that tells you that how -- the three letters have some meaning attached to them. So it means that if a file has a dot EXE extension, short for executable, then it can execute on your machine.

Q. Okay. And I think you used the word file extension?

09:47:59 **A.** That's right.

Q. All on the same page. What is a file extension?

A. File extension is the -- it's the letters that come after the dot. So in this case, you can see that it's dot EXE, but if you created a word document, it would say dot 09:48:15 DOC, or if you created a Power Point file, it would say dot PPT, or if you create a text file, it would say dot TXT. And it's a way to -- it's generally a three-letter abbreviation, and it's there to indicate what type of file you're looking at and also what the file is capable of 09:48:37 doing.

Q. Okay.

So the file extension appears after the file name?

A. Yes. It's three letters after a period, and the period and the three letters appear after the file name.

09:48:52 **Q.** So what happens if a user clicks on any executable and any dot EXE?

A. The file will run. It will execute.

Q. Okay. So if that happens to be the Trojan, the Bayrob Trojan, the Bayrob Trojan will execute?

09:49:07 **A.** Yes, that's correct.

Q. And what does that mean?

A. It means it runs and, you know, it does what it's programmed to do; connect to the Internet, passwords. It will start executing commands and start running.

09:49:19 **Q.** All right. Can we zoom back on this, Sue, for one minute? I just want to be clear.

So is there any reason -- any programming reason why a programmer would need to -- will call this file what it's called right here as translated into English?

09:49:39 **A.** No.

Q. That's just a personal choice?

A. Yes.

Q. Okay. Let's move to the next slide. Okay.

And these are translations of domain names, correct?

09:50:00 **A.** Yes, that's correct.

Q. And with the domain names, is there -- could that be anything as well and they're just picking particular domain names?

A. Yes, that's right.

09:50:10 **Q.** All right. Let's move to the next translation: Okay.

Here we see a translation, translates to, "Sucks webset." Can you explain what the significance of, "Sucks webset" is in the Bayrob Trojan?

A. Yes, it means that something went wrong when they were trying to execute their virus, and they're sending this 09:50:31

message back to the authors to tell them something went wrong.

Q. Gives them also information about what went wrong or just says, "Sucks webset"?

09:50:44 **A.** Gives them information about what went wrong.

Q. Okay. If we could scroll to the next page. All right. Thank you.

Now, was it significant to your investigation that there were Romanian words throughout the Trojan, throughout the code? 09:51:08

A. Yes, it was.

Q. How was that significant?

A. Well, it told me that the authors were likely Romanian.

09:51:15 **Q.** Okay.

And what -- could you tell what programming language the malware was written in?

A. Yes.

Q. What programming language was the written in?

09:51:27 **A.** In a program language called "C".

Q. Okay. What is "C"?

A. "C" is a way to write programs, to instruct the computer what to do.

Q. Is it a fairly popular programming language?

09:51:42 **A.** Yes, sir. It's very, very popular.

Q. Okay. As long as we're talking about programming languages, let me ask you a question. What is -- do you know what assembly language is?

A. Yes.

09:51:52 **Q.** What is assembly language?

A. A assembly language is a lower level representation of what a program is trying to do. So when you write "C" code, for example, it's very readable by the programmer. The programmer has to be able to write it. So it's very, you
09:52:14 know, it's a language and it's fairly easy to read.

Q. If you're a programmer?

A. If you're a programmer, and -- but when you convert that, when you actually convert that from the readable format into the EXE that we saw there, the actual file
09:52:30 that's going to run, and it no longer looks like the "C" language anymore, it gets converted into lower level instructions that are just numbers. But, the computer can understand those numbers. And the lowest level, lowest way to represent those numbers is what's called an assembly
09:52:54 language. It's another programming language. It's just a lot more difficult to write in and to understand and to read. And it's -- it was very low level and --

Q. Could you program an assembly language?

A. Yes.

09:53:13 **Q.** Is that something that's common for programmers to be able to do?

A. Yes.

Q. Okay.

A. I mean not really anymore. It used to be very common 09:53:24 to -- all programs used to be written in assembly language, but essentially better, easier languages have come along like "C" for example that are easier for programmers to write in. So generally, people try to write in the easiest language to write in.

09:53:39 **Q.** Today is it common to see someone write in assembly?

A. No, it's not common.

Q. Would most programmers know how to write in assembly?

A. Probably not.

MR. GOLDBERG: Objection.

09:53:50 MR. O'SHEA: Objection.

THE COURT: Sustained.

Q. In your experience, have -- do most programmers know how to write assembly?

A. No.

09:53:58 MR. GOLDBERG: Objection.

THE COURT: Sustained.

Q. Has Symantec caught programs that were written in assembly language as part of your work?

MR. GOLDBERG: Objection.

09:54:17 THE COURT: Overruled. You may answer that.

THE WITNESS: Very rarely.

Q. Okay. Was the Bayrob Trojan modular?

A. Yes.

Q. And what does it mean it say that the Bayrob Trojan 09:54:35 was modular?

A. It means that there was a base part of the virus that didn't change very much, but it could be extended or you could add functionality to it, via another piece, like a jigsaw puzzle. You could add more pieces onto it and make 09:55:03 it do more things without having to change the core of the virus itself.

Q. So one could add modules to it?

A. Yes.

Q. And when we're talking about one, are we talking about 09:55:16 who could add modules to it?

A. Well, the virus authors --

Q. The person who created the virus?

A. Yes.

Q. Okay. And how many different modules did you see 09:55:29 added to the Bayrob Trojan over time?

A. Around 50.

Q. Okay.

I'd like to show what has been previously marked as Government's Exhibit 1425. And this can be published to the 09:55:45 jury.

THE COURT: Do you have it up already, Sue?

MS. CHANDLER: I do not, your Honor.

THE COURT: I'm sorry?

MS. CHANDLER: I do not. My little thing is
09:56:20 scrolling and it's stuck.

THE COURT: Okay. Because we are not seeing anything, I just want you to know that.

MS. CHANDLER: Okay.

MR. LEVINE: While we're waiting, I'm going to
09:56:29 put it up on the Elmo, your Honor. Not seeing it here. I see it on the Elmo.

THE COURT: Folks, you can see it?

THE JURY: Yes.

THE COURT: All right.

09:56:59 BY MR. LEVINE:

Q. All right. We'll start at the top here.

Can you tell us basically what this is, Mr. Omurchu?

A. This is a listing of all the programs that I found that were used by the Bayrob Trojan, all the cellular
09:57:22 modules.

Q. How would the plug-ins end up in the malware? Were they there when the computer was infected or were they -- did they get there some other way?

A. No, they're there during the original infection. So
09:57:38 during the original infection, the Bayrob virus, the core

part of the Bayrob virus would be installed on your computer. And then after that, the commander control server would send instructions down to the infected computer and tell it to download these modules.

09:57:55 **Q.** Just so we're on the same page, you use the word plug-in's and you use the word modules. Are those the same things?

A. Yes, they're the same things.

Q. Okay.

09:58:04 So let's just take a look at the different columns here. What does the column to the left represent?

A. The name of the module, as I received it on my infected computer.

Q. Okay. So you didn't come up with those names?

09:58:20 **A.** No, I did not come up with those names.

Q. Those are the names that were in the malware itself?

A. Yes.

Q. All right.

And what does the second column, which says "times used," what does that represent? 09:58:30

A. That was the number of times that we saw this module distributed.

Q. From your infected computer?

A. From the traffic, yes, from the traffic that was coming through our infected computer. 09:58:51

Q. Okay.

And then category. What does -- what is that there?

A. That's an encryption of what the plug-in was trying -- high level description of what the plug-in was trying to do.

09:59:08 **Q.** Okay. And the next column seems to have some countries in it, what's that?

A. It's -- if the plug-in was -- the module was specific, doing something specific to a particular country, I marked that here in this column.

09:59:22 **Q.** Okay. If there's no country listed there, what does that mean?

A. It means it was specific to any particular country.

Q. Okay.

And what is the summary column there?

09:59:32 **A.** The summary is a brief description of what the plug-in does.

Q. Okay. And what is the source for this -- for all this information that you have here?

A. This was from my infected computer. So we could see 09:59:53 where these are being distributed from. So this is either from my computer, it was at -- my computer is asked to do something with this or we saw where this was being distributed and we were able to get it from there.

Q. Now, did you also see these plug ins stored on the 10:00:12 Bayrob Group's command and control server?

A. Yes.

Q. All right. And what was the name of the folder in which these were generally stored?

A. These are generally stored in a folder called DEP,
10:00:24 D-E-P.

Q. So that's D as in dog, E as in executable, and P as in program?

A. Yes.

Q. D-E-P?

10:00:33 **A.** Yes.

Q. Now, is that -- was D-E-P also the file extension for many or all of these plug-in's?

A. Yes, it was.

Q. And again what is a file extension?

10:00:49 **A.** A file extension is an abbreviation that tells you something about what the file can do.

Q. Okay.

Is -- so, for example, is PDF, dot PDF, is that a file extension for Adobe and Adobe PDF?

10:01:07 **A.** Yes.

Q. Is D-E-P a common file extension?

A. No.

Q. In your 14 years at Symantec, have you ever seen anyone, other than the Bayrob Group, use the D-E-P file
10:01:18 extension?

A. No, I have not.

Q. Never?

A. Never.

Q. Now many of these modules you have listed here also
10:01:27 seem to end in dot Casper in the end?

A. Yes.

Q. Dot C-A-S-P-E-R?

A. Yes.

Q. What is Casper?

10:01:36 **A.** Casper is -- Casper is a way to ultimate browsing of
web pages. So normally when you go to a web page and you
want to fill out a form, you go -- you have to go there
manually yourself, open the web page, go through the form,
fill in your name, and then click submit. And Casper is a
10:02:03 way to do that, is a way to ultimate that so you don't have
to sit there and do it. You can use Casper to do that for
you instead.

Q. And would that be happening, going out to the
website -- to a website and doing something in the
10:02:17 background of the computer?

A. Yes.

Q. So would the user ever experience it?

A. No, the user would never see that.

Q. All right. And is Casper, dot C-A-S-P-E-R, yeah, is
10:02:29 that a common file extension?

A. No.

Q. All right.

I'm going to show you what's been previously mark as Government's Exhibit 1426.

10:02:43 THE COURT: Where do you want it?

MR. LEVINE: We have to switch. I want to publish it to the jury.

Q. Okay. And I'm sure we'll have to zoom in at some part of this, but we'll get to that. All right.

10:03:02 So what is Government's Exhibit 1426?

A. This is a picture of the tool that we used to record traffic. It's called Wire Shark.

Q. Okay.

And is this showing Bayrob activity over one of your 10:03:19 infected computers?

A. Yes, it is.

Q. So okay.

So I just zoomed in on a portion of this. And is this -- well, let me ask it this. We see a lot of D-E-P 10:03:54 right here, a reference here. What does D-E-P mean in this context?

A. D-E-P is a folder name here, a folder where files can be stored.

Q. So these -- are there's files that are stored in the 10:04:13 D-E-P folder files that have a D-E-P extension?

A. Some of them have a D-E-P extension. In this case, yeah -- some of the files in there do.

Q. Okay. And we -- zoom in on this.

There is a D-E-P Casper J-S. It's line -- looks like 10:04:46 it's Line 141 here. Can you point the arrow to where it says Casper JS on your screen. Okay.

So what is that referring to?

A. That Casper JS is the program that allows you to ultimate visiting web pages. So what's happening here is 10:05:10 the eBay virus is downloading the Casper.JS file and that will enable -- it's like a module that will enable the Bayrob virus to now go and visit web pages and fill information into those web pages.

Q. So what's happening here is your infected computer is 10:05:33 being instructed to download the Casper JS file from the DEP folder?

A. Yes.

Q. Where is it downloading it from?

A. It -- it's downloading it from the command and control 10:05:46 server.

Q. If we can go back to Exhibit 1425. By the way, is Casper, is that a reference to the ghost, Casper the Friendly Ghost?

A. Yeah, it probably is a reference to that. I'm not 10:06:09 exactly certain.

Q. In what way, if at all, is the Casper file like a ghost?

MR. GOLDBERG: Objection.

THE COURT: Sustained.

10:06:31 **Q.** Going back to this 1425, one of the files here is called Casper Pipe towards the end. Do you see it towards the bottom there? Maybe we can move the -- there we go.

What is Casper Pipe?

A. Casper Pipe is a way to use the Casper program to control web pages. 10:07:07

Q. Okay. And that -- how would you -- how would you use Casper Pipe to control web pages?

A. So you give it instructions about how to navigate to web pages, what web page to visit, what instructions to 10:07:27 carry out on that web page, what information to fill in for that web page, and if -- whether you want to submit that web page, whether you want to record the results that come back from that web page.

Q. Okay. Let's go back to the big view here. And if we 10:07:48 could zoom in on the top. Okay.

So the first two modules you list here are put in the category of Click Fraud. What are those?

A. Click Fraud is a way for the virus authors to make money from showing ads. They don't actually show -- they 10:08:13 may not necessarily -- the user, infected user may not necessarily see the ads but the ads are -- it appears to the ad company that the ads have been shown to the user and the attackers can make money from having shown those ads.

Q. So who does the attacker get the money from?

10:08:32 **A.** From the advertising company.

Q. All right.

So there's an advertising company that pays people for distributing ads?

A. Yes, exactly.

10:08:39 **Q.** And this is -- these modules are a way of distributing ads and getting money from the ad company?

A. Yes.

Q. And the user never necessarily sees those ads?

A. No, this would all happen silently in the background. 10:08:57 So even though your computer looks like it's working normally, invisibly to you, in the background it's actually visiting web pages. And when it visits those web pages, it has the opportunity to click on ads, to see ads and click on ads. And even though you won't notice any of this, but to 10:09:15 the advertising company, it would look like you were -- you were, you went, visited that web page, you saw that ad, and you clicked on that ad.

Q. Okay.

The next file is Minor Force, what was Minor Force?

10:09:28 **A.** Minor Force is a way to make sure that a certain module on your computer was always running.

Q. Okay. And what did that module that was always running, what was that module?

A. That module was mining for Cryptocurrency.

10:09:46 **Q.** So we're going to have to step back here and go slow because -- can you explain, first of all at very general level, what is Cryptocurrency?

A. Cryptocurrency is a form of digital money.

Q. Form of digital money?

10:10:04 **A.** Um-hum.

Q. So it's exchanged over computers?

A. Yes, exactly.

Q. All right.

And you talked about mining for Cryptocurrency. What is that? 10:10:17

A. So to create coins in a Cryptocurrency, you need to do some work to create that coin, like gold mining. For example, you need to go into the mine and you need to dig through the ground, you need to do some like difficult work in order for extract the gold. 10:10:37 It's the same for Cryptocurrencies, digital currency. And on your computer, you need to solve some difficult equations and different mathematical equations. And the way you prove that you can get a coin is by supplying the answer to those difficult equations. 10:10:59

So you have to prove that you did a lot of work on your computer in order to gain a coin.

Q. All right.

I understand why with mining you need to do a lot of work to get the gold. 10:11:10

A. Uh-huh.

Q. Or whatever you're mining for. Why do you have to do a lot of work to get Cryptocurrency?

A. It's designed in that way. The currency is designed in a way where it's difficult for you to generate a coin to 10:11:25 create a coin, and the way you create a coin is by solving very difficult mathematical equations, and you can use very fast computers or a lot of computing power in order to do that.

10:11:46 So the reward you get for putting in all of that work and all that effort is you get rewarded with a coin.

Q. You keep referring to a coin. Are you talking about a real coin in real world or are you talking about a digital currency?

10:12:00 **A.** A digital currency. A digital coin exists only on your computer.

Q. Okay. So how does one -- or can one make money from mining for Cryptocurrency?

A. Yes.

10:12:16 **Q.** How does one make money by mining for Cryptocurrency?

A. So in a normal case, what you do is you run a program on your computer that tries to solve these mathematical equations. And if you happen to solve one of these equations, you submit your answer. And in return for having 10:12:38 a correct answer, you get given something of value, a coin. And then you can trade that coin or you can convert that coin into US dollars.

Q. Okay.

Now, what would a person need in order to be effective 10:12:55 at Cryptocurrency, mining for Cryptocurrency?

A. Well, you need a lot of power, computer power to try and solve these mathematical equations.

Q. So would you need a botnet, a large series of infected computers?

10:13:12 MR. GOLDBERG: Objection.

Q. To do Crypto mining?

THE COURT: Overruled. You may answer that, sir.

THE WITNESS: Yes, yes.

10:13:20 **Q.** Okay.

So is there -- is there any other way to effectively Cryptomine besides having a large number of computers?

A. You need a lot of processing power. So one way to have that processing power is to have a lot of computers 10:13:38 work for you. So yeah, you need a lot of computers doing work.

Q. Okay.

So one way would be to have a large number of infected computers doing work for you. Say I was in China. Is there another way if I was in China that I might Cryptomine? 10:13:49

A. Yes.

Q. How would I do it in China?

A. In China, there are people, companies, that have data centers set up. And inside those data centers are warehouses. 10:14:03 They have lots and lots of computers set up, running that are trying to solve these mathematical equations. And they're doing it as an enterprise to make money. So they have a large number of computers in one location, trying to make money for them.

10:14:23 **Q.** Okay. So let's just break that down a little bit. What's a data center?

A. It's a warehouse where you have -- you have computers that you can use for whatever you choose.

Q. And are we talking about thousands of computers usually? 10:14:40

A. Yes.

Q. Okay.

And why is this a method of Cryptocurrency mining that's particular to China?

10:14:54 **A.** Well it's not particular to China, per se. You can do it anywhere in the world but in China, it is -- it is known that companies in China do this, perhaps because of the economics.

Q. Is the energy costs cheaper in China for purposes of doing this? 10:15:16

A. Yes. So the energy cost is lower, wages are lower, the price of hardware is lower. Generally, the computers are built in China. So they're cheaper to transport to the location as well. So all of those work in the favor of doing this in China. 10:15:36

Q. Is Cryptomining or Cryptocurrency mining very power intensive?

A. Yes, it is.

Q. Okay.

10:15:49 So in order to be effective at Cryptomining, we mention two possible ways: Having a big data center pull full of computers or controlling a whole bunch of infected computers?

A. Yes.

10:16:02 **Q.** Now, was one of the things that you witnessed on your infected computers Cryptomining?

A. Yes, it was.

Q. And what effect did you see Cryptomining have on the infected computers that you were monitoring?

10:16:16 **A.** It made them run very slowly.

Q. Okay.

And was that all the time or just when the Cryptomining program was launched?

A. It was just when the Cryptomining program was running. 10:16:28 So when the Cryptomining program was running on your computer, it was using a lot of the power, processing power in your computer. So it wasn't a lot left over for doing other things like, you know, running Word or browsing the web or anything else you might want to do on your computer. 10:16:47 What I noticed was that my computers run very slowly.

Q. I know it's hard to quantify, but how slow would you say it was running? How did it actually impact you?

A. Extremely slowly. In some cases, it was so slow that I couldn't connect to my computers anymore.

10:17:04 **Q.** Okay.

And, in fact, did you have to -- what did you do in order to continue using some of those computers that were running that slowly?

A. I stopped the Cryptomining program from running or I 10:17:21 limited the amount of processing power that that program could take up.

Q. How were you able to stop it from running?

A. Well, if you know the name of the file, you can remove the file from your computer or you can find the file that's 10:17:39 running and you can issue a command for it to stop.

Q. Is that something a normal infected user would be able to do?

A. No.

Q. Did you at any time -- did you have to install a 10:17:50 program to stop the mining and be able to continue the monitoring?

A. Yes, I did.

Q. And why did you do that?

A. Because it was becoming very difficult for me to 10:18:00 monitor what the virus was doing because the computer was running so slowly that I wasn't able to run my monitoring software.

Q. Okay.

Were these fast high quality computers that Symantec 10:18:12 was monitoring?

A. Yes.

Q. But they still basically became unusable when they were being directed to mine for Cryptocurrency?

A. Yes.

10:18:24 **Q.** Now when your computer was being directed to mine for Cryptocurrency, you said the money could be generated; is that correct?

A. Yes, that's correct.

Q. Did you get that money?

10:18:36 **A.** No.

Q. Who would get that money?

A. The Bayrob authors.

Q. Okay.

Looking back at 1425, what does the 22,022 number mean
10:18:50 next to Minor Force there on the third line?

A. It means the amount of times that we saw that command being issued, that module being used.

Q. Okay.

And so what does that mean happens 22,000 times?

10:19:09 **A.** So what Minor Force does is it ensures that the mining, the Cryptomining program is running on the computer so that the Bayrob Group wanted to have the program running as often as possible so that they could make as much money as possible from that, so they would continuously force the
10:19:29 program to run if it had shut down or had some problem or, you know, there was some other problem encountered. This was a way for them to make sure it was always running.

Q. Okay.

And was that on all the 22,000, was that on all your
10:19:46 systems or was that on other infected systems as well?

A. It was both.

Q. Both your infected systems and other infected systems?

A. Yes.

Q. And this is what you saw?

10:19:56 **A.** This is --

MR. GOLDBERG: Objection.

THE WITNESS: This is only a very small portion of the full activity that was happening on all infected computers.

10:20:03 MR. GOLDBERG: Objection.

THE COURT: Sustained.

THE WITNESS: We didn't have --

THE COURT: Sustained.

BY MR. LEVINE:

10:20:09 **Q.** Was this -- did you have full visibility into what was going on with all infected computers or did you have a limited visibility?

A. We had limited visibility.

Q. How was your visibility limited?

10:20:20 **A.** We could see what was happening on our own infected computers, and we could see the traffic, the instructions that were being sent across our infected computers.

Q. Okay.

And was the 22,022 number, was that as of a particular 10:20:38 date? I'm not asking you what the date is. Was it as of a particular date?

A. Yes, it was, yes.

Q. So if you had -- if you could continue to monitor beyond that, if that number would have presumably increased?

10:20:53 **A.** Yes.

MR. GOLDBERG: Objection.

THE COURT: Overruled. I'll allow it to stand.

Q. Okay.

10:21:00 Now looking towards the bottom of Government's Exhibit 1425, there is a module called Burst Zap. If we could zoom in and maybe -- if you could please highlight. Thank you so much.

What did the module Burst Zap do?

10:21:28 **A.** I may need to explain what Burstcoin is. Is that okay?

Q. Yes. Let's step back. What is Burstcoin?

A. So Burstcoin is another type of digital currency but it's generated in a different way from what I talked about previously. 10:21:46

Q. Okay. Just -- so there's different Cryptocurrencies then?

A. Yes, that's right.

Q. Can you name some Crytocurrencies?

10:21:56 **A.** Yes, Bit Coin is the most current Cryptocurrency.

Q. And you're saying Burstcoin is the name of another digital currency?

A. Yes.

Q. How is Burstcoin different from Bitcoin?

10:22:09 **A.** So Bitcoin is either the coins are generated in the way that I mentioned earlier. You need to solve difficult mathematical equations using power on your computer. So your -- the computer needs to run and do a lot of work. You need to prove you've done a lot of work to get the coin.

10:22:34 With Burstcoin, you don't need to do that. With Burstcoin, what -- instead what you do is you use this the space on your computer, the spare space that has not been used. You fill that up with tables that can be used to solve these mathematical equations. So instead of having to 10:22:52 run your computer and have your computer be very slow, which a lot of people don't like to do, instead you can use the spare space on your computer, which you weren't using anyway, and you can use that to help you generate coins, Burstcoins.

10:23:09 **Q.** Okay.

So it's another coin and can you make money from mining Burstcoin in the same way that you could with the other coins --

A. Yes.

10:23:21 **Q.** -- you talked about? Okay.

So with that background, can you explain what the module Burst Zap did?

A. So Burst Zap deletes all files that are in the recycle bin.

10:23:34 **Q.** What is the recycle bin?

A. Recycle bin is the place where when you delete a file from your computer, it goes to the recycle bin.

Q. I'm sorry.

A. So that if you need to recover it, at some point in 10:23:48 the future, you can recover it. So it's not completely gone. It's gone from where you were storing it before, but it's now in the recycle bin. And then at some point, if you discover you didn't want to delete it, you can go in there and get it back.

10:24:01 **Q.** So is it like putting something in the waste basket but not actually emptying out the waste basket into the real trash?

A. Yes.

Q. And is that the icon on the screen that looks at you 10:24:14 like a little waste basket?

A. Yes.

Q. And I guess I should say what is an icon?

A. It's a little picture.

Q. Picture that appears on the computer?

10:24:25 **A.** Yes.

Q. And what happens when you click on an icon?

A. Some action happens for recycle bin. It would open the location so you can, you could see the files inside the recycle bin.

10:24:36 **Q.** Okay.

So you said that the Burst Zap module removes certain files from the recycling bin?

A. That's right.

Q. What files does it remove from the recycling bin?

10:24:48 **A.** It removed all files that are in the recycle bin.

Q. So what does that have to do with, if anything, with Burstcoin?

A. So when you use -- one of the problems with Burstcoin is that it uses up all your available space, and I am -- 10:25:08 your computer -- you want to store more files, you may not have space. So if you deleted files from your computer, they would go into the recycle bin but the space is still taken up on your computer.

And if you remove the files from their recycle bin, 10:25:21 then space becomes available on your computer again.

Q. Okay.

Was the Burstcoin mining activity or file space that was being used, was that stored in the recycle bin?

A. From the Burst Zap module, because it was related to 10:25:42 Burstcoin, it appears that they wanted to empty the recycle bin, either to make more space upon your computer or to remove some of their files that they created.

Q. Okay.

So it may be to remove files that they created?

10:25:58 **A.** Yes.

Q. Why would they want to remove files that they created?

A. To either stop what they had done or to make more space.

Q. Okay.

10:26:08 Going back to the top of the list, if we could just highlight the ones -- all right. So many of these -- many of these files are put in the category of crawler, any of these modules. What is a crawler?

A. A crawler is a program that will visit lots of 10:26:44 different web pages and generally scrapes the web page for some information.

Q. Okay.

So is the Florida Bar scanning example that we looked at earlier, was that an example of a crawler?

10:27:00 **A.** Yes.

Q. What other crawler modules did you identify here?

A. Lots of different modules. For example, Trip Advisor, there's a module here to go to Trip Advisor and to crawler and extract contact information.

10:27:18 You can see Yellow Pages in various different language. Down at the bottom there, you have a Yellow Pages. And if you go up here, this is the Arab Emirates Yellow Pages website. And this is Páginas Amarillas is Spanish for the Yellow Pages. And Pages Jaunes just above 10:27:45 that, that's French for Yellow Pages. So there was lots of different modules sent down that would allow the Bayrob virus to scrape information from different web pages.

Q. So these modules would have your infected computers or anyone's infected computers going out and scraping 10:28:06 information from websites?

A. Yes.

Q. Why would someone have the infected computers do that rather than just doing that themselves?

A. Well, to distribute the work across many different 10:28:15 computers, and then also to make sure that the -- if you did it from one computer, you would probably get band making too many requests to the one website.

So if you distributed it over a large number of computers, it's less likely for the website owner to 10:28:32 understand that you are just sucking information from their website.

Q. So in other words, if I was the owner of YellowPages.com and I saw that one computer was going to every single page rapidly over a short period of time, so 10:28:52 what might the owner of YellowPages.com do?

A. Likely ban that computer from that activity.

Q. How do they do that?

A. They would look at the address of the computer and they would put a block in for that address.

10:29:07 **Q.** Okay.

THE COURT: I'm going to interrupt at this point in time.

Folks, we're going to take our morning recess. Please remember the admonition.

10:29:16 And for your information, one of the attorneys has a commitment today at noon. So we will take a luncheon break from noon to 1:00 today.

All rise for the jury.

(Thereupon, a recess was taken.)

10:49:13 THE COURT: You may continue.

MR. LEVINE: Thank you, your Honor.

BY MR. LEVINE:

Q. Mr. Omurchu, one of the files, the modules, the plug-in's we had already talked about on the screen here is 10:49:25 Minor Force?

A. Yes.

Q. Do you recall that?

A. Yes.

Q. And you testified that Minor Force helped facilitate, 10:49:34 helped make possible the mining of Cryptocurrency?

A. Yes.

Q. You recall that?

The file name Minor Force, have you seen that anywhere else besides in the Bayrob Trojan?

10:49:47 **A.** No, I have not.

Q. Okay.

And just for context, when I ask you if you've seen a file anywhere else, can you tell me about Symantec's collection of malware? How many malware samples and virus 10:50:03 samples do you have access to?

A. Millions.

Q. Millions?

A. Yes. We receive actually millions of malware every year and we store all of that malware. So we have, you 10:50:16 know, years and years and years of collections of malware.

Q. Okay.

So when I asked if you've seen Minor Force or DEP as a file extensions anywhere else, you haven't seen it in any of those million of file samples other than the Bayrob?

10:50:35 **A.** Exactly.

Q. Okay.

So we had talked a little bit about these crawlers, and I want to now zoom out and zoom in on another category you have here called Info Stealer. So if we could zoom in 10:50:49 on the category that you call Info Stealer.

And what is an Info Stealer?

A. It's something that steals information from your computer.

Q. Okay.

10:51:02 What types of information would these modules steal from your computer?

A. They would steal a variety of different information from your computer. But, then the names of the modules kind of give you an idea of what they were stealing. So, for 10:51:17 example, the first one is Browser Passwords. So that module is trying to steal passwords that are stored in your Internet browser.

Q. Let's stop there for a second.

Are passwords stored in your Internet browser?

10:51:32 **A.** Yes. So if you want to visit a website frequently, let's say your e-mail website, instead of you having to go type in your user name and a password every time you go there, you can have them stored in the browser to make it easier for you. When you revisit that web page the next 10:51:52 time, you can just click enter and the information will get populated into that web page automatically so you don't have to type it every time. And to facilitate that, they store your password in the browser.

Q. Now to be clear, if I have an e-mail account at 10:52:15 yahoo.com, and I also have another e-mail account at gmail.com, and I went into Yahoo and I stored it to enter my gmail account password or user name or password, which I've never entered into the Yahoo browser before, would that be stored there?

10:52:34 **A.** So it stores the website that you visit and the credentials that you use, the user name and password you used at that website so they're associated together. So in the browser, they will have Yahoo mail, and then they'll know your user name and your password for Yahoo mail. So if 10:52:52 you start to type in the user name for Yahoo mail, they can fill the rest in for you. And then if you went to gmail or some other site, and you started typing the user name there, the browser understands that you're on a different web page and it can go and it can take out the user name or password 10:53:14 that's correct for that web page.

Q. So, in other words, if I start to enter my gmail address into Yahoo, and I've never entered that gmail address into Yahoo, it's not going to auto populate that?

A. No.

10:53:28 **Q.** You're saying correct? Just --

A. Correct.

Q. -- just for the record. Okay.

So what this module would do is steal all those user names and passwords that your browser is remembering?

10:53:42 **A.** That's correct.

Q. What other type of information would these modules steal?

A. They -- so, for example, the second one on the list here, buletine, I believe that's the Romanian word for 10:53:56 passport or -- yeah, passport. And this was trying to steal passport pictures for documents that were stored on your computer.

Q. How would a program know that something was a passport picture or passport document on your computer?

10:54:12 **A.** It searched for the file names, passport, and/or buletine, and if it found documents that matched that file time, it would send them to the attackers.

Q. What other information stealers did they have here?

A. Outlook accounts that could collect e-mail addresses 10:54:35 from your Outlook account.

Wallets dat is another one. That would steal your digital currency wallet so when you have coins in digital currency, they're stored in a wallet on your computer, and this Info Stealer was able to steal that wallet, essentially 10:55:00 steal your digital money.

Q. If you deal with Cryptocurrency, you have a wallet on your computer?

A. Yes.

Q. Like this?

10:55:13 **A.** Yes, exactly like that, except it's on your computer. And if you open up that wallet, inside that wallet are your coins.

Q. All right. And just for the record, I was holding up my physical wallet. Don't ask. It's like this.

10:55:26 So what this would do, what this module would do is steal all the coins in the wallet?

A. Yes.

Q. Okay.

What other information stealers do they have in these modules? 10:55:38

A. They could steal the user name and password for your Wi-Fi, your wireless Internet connection.

Q. What would the value of the user name and the password to your Wi-Fi be?

10:55:56 **A.** I'm not sure what it was being used for but --

MR. O'SHEA: Objection.

THE COURT: Sustained.

MR. LEVINE: His answer is he doesn't know.

THE COURT: Excuse me.

10:56:06 MR. LEVINE: Sorry.

Q. Okay.

What other -- and were there any other information stealers you saw there?

A. There's another module there that would collect the information about what was running on your machine, what 10:56:21 files were executing on your machines so they could know what the -- all of the processes were on your machine or all the files that were running.

Q. And what is a process that would be running on one's machine? 10:56:38

A. When a file is running on a machine, it's called a process.

Q. So like if I'm running Microsoft Word, is that a process?

10:56:45 **A.** Yes.

Q. Okay. All right.

Let's take a look at Government's Exhibit 1427, please. What is Government's Exhibit 1427?

A. This is a picture I took of -- on my infected computer 10:57:15 of when I visited Facebook.

Q. Okay. And what happened, what did you see when you visited Facebook?

A. So when I visited Facebook, instead of getting the normal log-in page, I got this security prompt instead and 10:57:33 telling me that I needed to complete a security check in order to log into Facebook.

And this content that I'm seeing here asking me to enter my credit card to verify my account, and this content is not coming from Facebook, even though in the URL bar at 10:57:51 the top says www.facebook.com up here, so it looks like the real Facebook website, but the content that you're seeing here is not coming from Facebook.

Q. Where is it coming from?

A. It's coming from the Bayrob virus.

10:58:06 **Q.** Okay.

Let's look at the second page of this exhibit. What are we seeing on the second page here?

A. So I scroll, this is a picture I took of the bottom half of that page. The page was long so I just scrolled 10:58:21 down and I took a picture of the bottom half of it. And you can see here, the fields that it's asking you to fill in your name and then your credit card number, and expiration, date, and CVC number, and this is -- it's meant to verify your account with Facebook.

10:58:45 **Q.** Okay.

So is that information we see there in full name, address, the information we see typed into these fields, where do those come from?

A. That's information that I typed into those fields.

10:58:58 **Q.** So is that all fake information?

A. Yes, it is.

Q. And then what would happen if you clicked "confirm identity" at the bottom?

A. When you click "confirm identity," this information is 10:59:10 sent to the command and control server.

Q. Okay. Can we go to the next page, Sue? Thank you so much, and if we could yes please zoom in on that.

What is this showing, Mr. Omurchu?

A. This is showing the information being sent back to the 10:59:28 command and control server.

Q. When you say "it," what is sent back to the command and control server?

A. The -- so the credit card information I just entered into the previous page, when I click submit, this is the 10:59:44 request that is sent. This is the information that is sent back through the command and control server. And you can see that it says the type is CC. That stands for credit card. And the mode is Facebook, signifying the credit card has been stolen while pretending to be Facebook.

11:00:01 **Q.** Okay. Is this screen that we see right now, is this something an ordinary user would see when they hit confirm?

A. No.

Q. How are you able to see it?

A. I was able to see by using the auditing tools to 11:00:16 monitor requests being sent.

Q. Okay.

Can we see the next page, please? All right. What is -- what do we see here on Page 4 of Exhibit 1427?

A. So this is a -- this is a page that is pretending to 11:00:35 be Wal-Mart or attempting to -- it's a copy of the Wal-Mart web page that the Bayrob Group was using to try to convince people to purchase something.

Q. And could we -- look at the next page, please. What do we see here on Page 5 of Exhibit 1427?

11:01:03 **A.** So here I've clicked on one of the items for sale, and

I've gone in to that page. And you can see there's a "proceed to check out" button.

Q. And then is it -- let's take a look at the next page. Is -- what is this page?

11:01:18 **A.** This is the -- this is the check out page. This is where you would buy the item. In this case, it's a tablet, computer tablet, and it's asking for my credit card information to confirm the purchase.

Q. And what happens if you put in credit card information? 11:01:37

A. That information gets sent to the command and control server.

Q. All right. Look at the next page. Let's look at the -- this is a -- what is this?

11:01:49 **A.** This is -- a fake credit card number that I -- that I typed in and fake information I typed in. Then I typed this information in, in order to see if this information would get sent to the command and control server when I click continue.

11:02:04 **Q.** And did it get sent to the command and control server?

A. Yes, it did.

Q. Let's take a look at the next page, please. And let's zoom in on that. What does this page show?

A. Again, this is the request -- this is the data that is sent to the command and control server when I click confirm 11:02:19

on the purchase page. And again, you can see that the type is CC for credit card. And in this case, the mode is AOL for Wal-Mart, and the page was pretending to be Wal-Mart.com.

11:02:37 **Q.** Now did the Bayrob Group have a way to record and organize all this information that it was getting from victims?

A. Yes, it did.

Q. How did the Bayrob Group do that?

11:02:47 **A.** They would store it on the command and control server.

Q. I'm showing you what's been marked as Government's Exhibit 1428. And if we could zoom in on the next there. Thank you.

What is Government's Exhibit 1428?

11:03:07 **A.** These are credit card numbers that were stored, that were stolen and stored on the command and control server.

Q. Okay.

And is this just credit card numbers or additional information?

11:03:24 **A.** There's additional information here. There's the name, the address, the state, the telephone number, expiration date, e-mail address, yeah, a lot of information there.

Q. And amongst the information is the credit card number?

11:03:46 **A.** That's correct.

MR. O'SHEA: Objection.

THE COURT: Overruled.

Q. And where did you obtain this?

A. I obtained this from the command and control server.

11:03:55 **Q.** Now, is this -- what kind of -- is this a text file?

A. Yes, it's a text file.

Q. What is a text file?

A. A text file is a file that only contains readable information.

11:04:08 **Q.** Only readable information?

A. Text.

Q. Only text?

A. Yes.

Q. And is there a particular file extension for a text file? 11:04:14

A. Yes. At the top here, you can see that this file is called CC, short for credit card.txt, and txt is the extension for text.

Q. Did you make up that name, CC.txt?

11:04:31 **A.** No, I did not.

Q. Is that how it was named on the command and control server?

A. Yes, it was.

Q. All right.

11:04:41 Now, through your infected computers, did you witness the Bayrob Group sending any encrypted e-mails amongst themselves with subject lines containing CC or attachments named CC?

A. Yes, I did.

11:05:01 **Q.** All right. Let's look at Government's Exhibit 1428, please. That's what we're looking at right now. All right.

If we can look at Government's Exhibit 1429. Thank you. Thank you very much, Sue. I appreciate it. All right. What are we looking at here?

11:05:30 **A.** So this is a reconstruction of the command and control server, page stored on the Bayrob command and control server.

Q. What page is this?

A. This is the credit card page.

11:05:46 **Q.** Okay.

And is this a database a spreadsheet? What are we looking at?

A. This is -- this is a record of all of the credit cards that are available for the Bayrob Group that have been 11:06:05 stolen by the Bayrob Group and are available to be used and by the Bayrob Group. So on the left column here, these are the victims and the victim information, their address and their bank information. And then that's in the column line. And then in the next column over and then notes column is a 11:06:30 note that has been made about that particular credit card.

And then on the right column, there's ways to -- for the people who are using this web page and the Bayrob Group to be able to update the information there or deletes the information.

11:06:48 **Q.** All right.

So to be clear, when you say the people using this page, who is using this page?

A. The Bayrob Group.

Q. Okay.

11:06:59 Is this visualization of the -- with a line section, with an address section, and a note section and an action section, did you create this organization or is that something that the Bayrob Group created?

A. No, I did not create this. This is what the Bayrob Group created. 11:07:17

Q. Okay.

Oh, that white box that's to the left there, is that in the original or is that a redaction?

A. That's a redaction. That has the victims' names in there. 11:07:36

Q. So that has been redacted for the victim's privacy?

A. Yes.

Q. Now, other than that, the redaction of the victim names, is this a fair and accurate screenshot of the page you saw from the command and control server? 11:07:51

A. Yes, it is.

Q. What is the title of this database or program?

A. It's CC.

Q. All right.

11:08:10 And there's a column there towards the left that says good, and some of them are checked and some of them are not. Do you have any understanding what that means?

MR. O'SHEA: Objection. Well, let me ask you, sir, if you would answer it yes or no only.

11:08:32 THE WITNESS: Sorry. What was the question again?

BY MR. LEVINE:

Q. The question was do you have any understanding of what that good column means with check boxes and some are checked and some are not? 11:08:42

A. Yes.

MR. LEVINE: May I proceed, your Honor?

THE COURT: What's the basis of your understanding?

11:08:50 THE WITNESS: Notes that were left in the note column in this page.

Q. Okay.

So what does -- what does it mean where it's checked good or it's left unchecked?

11:09:03 MR. O'SHEA: Objection.

THE COURT: Overruled. You may answer.

THE WITNESS: My understanding is that these credit cards are able to be used at the moment.

Q. So if it's checked good, it's able to be used at the moment? 11:09:15

A. Yes, it's being confirmed good.

MR. O'SHEA: Objection.

THE COURT: Well, sustained. Sustained. I am going to strike that -- the last couple of answers regarding this issue. 11:09:24

BY MR. LEVINE:

Q. All right. What does the notes field refer to?

A. The notes field refers to actions that have been taken by the Bayrob Group with that credit card.

11:09:38 **Q.** Okay.

And we'll see a translation of that in a moment. But, does this screenshot show the entire CC file at a particular time or just part of it?

A. Just part of it.

11:10:00 **Q.** And on just this one part of the CC table, how many times do you see the moniker "Minolta" up here?

A. One, two, three, four, five, six, seven, eight, eight times.

Q. Okay.

11:10:21 And does the CC dot text file that we just looked at, which looked more or less graphable, does that somehow get ingested into this more graphical table?

A. I believe so, yes.

MR. GOLDBERG: Objection.

11:10:37 THE COURT: Sustained. That will be stricken.

Q. Do you know whether the CC text file gets ingested into this table?

A. I don't know for certain.

Q. Okay. Let's -- if we can look at Government's Exhibit 11:10:57 1430.

What is Government's Exhibit -- if you can zoom in on just the text part of this document. Thank you so much, Sue. What is Government's Exhibit 1430?

A. This is a log that was stored on the command and 11:11:22 control server. It's a screenshot I took of a log.

Q. Okay. And is this a text file also?

A. Yes, it is a text file.

Q. Okay. And what does it contain?

A. It contains information that had been stolen from 11:11:39 victim computers.

MR. O'SHEA: Objection.

THE COURT: Sustained.

Q. Do you know -- what is the source of your information about what this file contains?

11:11:51 **A.** On my computer, I monitored information that was sent from my computer when information was stolen. For example --

MR. O'SHEA: Objection.

THE COURT: Overruled. Continue, sir.

11:12:05 THE WITNESS: For example, the Bayrob Group, Bayrob Trojan was able to use passwords when the victim on the computer tried to log into the website, for example, eBay. And when that user's name and password was stolen, it was sent to the command and control server.

11:12:20 **Q.** Okay. And were you able to see some of those user names and passwords you witnessed being stolen from your infected computers on these tables?

MR. O'SHEA: Objection.

THE COURT: Overruled.

11:12:31 THE WITNESS: Yes.

Q. And is that how -- is that one of the ways you know what this table represents?

MR. O'SHEA: Objection.

THE COURT: Sustained. Rephrase your
11:12:43 question.

BY MR. LEVINE:

Q. So based on what you described, what does this table represent?

A. So when --

11:12:51 MR. O'SHEA: Objection.

THE COURT: Overruled. Go ahead.

THE WITNESS: The Bayrob -- when the computer was infected with the Bayrob computer and you went to log into eBay, it would steal the user name and password and 11:13:17 then they would take that user name and password and they would put it into a message that looked exactly like the message that is stored in this log file with the "pass equal to" and "keep me signed in" option. Those -- that text is text that was embedded in the Bayrob virus. So that's text, 11:13:33 I would see that text being sent from my computer to the command and control server.

Q. Okay.

So let's go through these lines. What does the e-mail address line here represent then?

11:13:45 **A.** This is the e-mail address of the victim.

Q. Did they -- the victim put in where --

A. So every time the Bayrob virus was being sent to a victim, the creators of the Bayrob virus would put the e-mail address of the victim into the virus itself. So by 11:14:06 examining the virus, I could see who the victim was by looking at that e-mail address. So this is the e-mail address that was embedded in the virus.

Q. Okay. And the next line says LICI. Do you know what that line is about?

11:14:22 **A.** That's an abbreviation for the Romanian word "auction."

Q. Okay.

And what auction, like an auto auction on eBay?

A. Yes.

11:14:33 MR. O'SHEA: Objection.

THE COURT: Sustained, form of the question.

Q. And what do you mean by auction?

A. So the original eBay virus was trying to convince victims to buy a car on eBay. And to do that, they would 11:14:53 show images of a car and then they would -- when you visited eBay, they would intercept that and show you a car that didn't exist. And the way they were able to record which virus was trying to sell which car was that they would put in this term LICI, L-I-C-I, and after that, after that, they 11:15:17 would have an abbreviation for the type of car that was being sold.

Q. Okay.

So that we see after that an abbreviation for type of car being sold?

11:15:29 **A.** It's two things. It's -- in this particular case, I don't know what this particular one is, but from my analysis, it shows the abbreviation of the Bayrob virus member who was trying to do the scam, and then after that --

MR. O'SHEA: Objection.

11:15:44 THE WITNESS: -- it shows --

THE COURT: Overruled. Go ahead.

THE WITNESS: After that, it shows an abbreviation for the car that was being sold in that auction.

11:15:51 **Q.** Okay.

And when you say the abbreviation that Bayrob member, you mean the abbreviation of the actual name in the real world or an abbreviation of the moniker that they used?

A. An abbreviation of the moniker they used.

11:16:06 **Q.** And after that is an IP address. What -- what does that represent?

A. That's the IP address of the victim's computer.

Q. Okay. And what is -- S-O-X, SOX ID?

A. So that is the ID of the proxy on the infected 11:16:25 computer that the Bayrob Group could use to log into that computer.

Q. So, if the Bayrob Group wanted to log into another computer, to an infected computer, they would enter that SOX ID for the infected computer?

11:16:46 MR. O'SHEA: Objection.

THE WITNESS: Yes.

THE COURT: Sustained to the form of the question.

Q. Can you explain how the Bayrob Group member would use 11:16:53 that SOX ID in order to log into an infected computer?

A. Yes. That SOX ID uniquely identifies the infected computer. And by using that SOX ID, the Bayrob Group would be able to -- actually a combination of the IP address above and the SOX ID, they would connect to that address and they 11:17:12 would use that SOX ID to be able to access the computer remotely.

Q. And what does the log-in info line at the bottom there show?

A. So the log-in info is the information that was stolen 11:17:26 from the victim when they attempted to log into a site.

Q. Okay. So what does that log-in information include?

A. It includes a user name and the password. So in this case, the user name is CK under score, marine under score, 1. And the password is Sniper 99.

11:17:51 **Q.** And what does "keep me signed in option equal one" or just "keep me signed in" --

A. There was an option that would allow you to stay logged in so you didn't have to re-sign in every time, and that's an indication of that status.

11:18:07 **Q.** Okay.

Can we go back now -- before we go back, is this -- is this something that is generated automatically by the virus or something that one would have to enter in manually?

A. This is something that's generated by the virus, and 11:18:28 each entry that you see here is generated from a different log-in attempt, and the information here tells you what computer the information came from and what was the user name and password used on that individual computer. And the virus generates this and sends it to the command and control 11:18:44 server.

Q. And then what happens to that individual record once it's sent to the command and control server?

A. It's stored on the command and control server.

Q. In the form of this exhibit?

11:18:55 **A.** Yes.

Q. Okay. Let's go back to Exhibit 1425, please.

THE COURT: Did you say 25? 1425?

MR. LEVINE: 1425, yes.

BY MR. LEVINE:

11:19:21 **Q.** All right.

So you have one file listed here called scam or rather you categorize as scam and the file is called or the module is called Browser Load, what is that file?

A. So this allowed the Bayrob Group to send a message to 11:19:40 the infected computers to open the browser and to load a specific web page.

Q. So can you give an example of that?

A. So, for example, in the case of Bayrob, if they wanted to try to scam a victim, they could have the browser pop up 11:20:04 with an offer, a web page that was an offer, and that would entice the victim to interact with that web page and maybe buy something on that web page.

Q. So this is what's sometimes referred to as a pop up?

A. Yes.

11:20:17 **Q.** If we could take a look now, zoom out and look at the ones called scammer, the lines. So you have a category called Spammer. What do the Spammer modules do?

A. The Spammer module allowed the infected machines to send spam, unsolicited e-mail.

11:20:45 **Q.** It would send spam from the infected computers?

A. Yes.

Q. And what would they send the spam through, what e-mail source?

A. They would use AOL, AOL e-mail accounts to send the 11:21:01 e-mails.

Q. AOL? Are all these AOL?

A. There's AOL Spammer and the AOL tester.

Q. Also an Outlook one that they had?

A. Yes.

11:21:16 **Q.** All right.

So if I was a Microsoft Outlook user or an AOL user, let's start with Microsoft Outlook -- what would this module do to my computer if I was infected?

A. It would try to send e-mail from your Outlook account.

11:21:34 **Q.** Who would it send that e-mail to?

A. It would take -- it would take the context -- contacts from your Outlook program and try to send spam to all of the contacts in your Outlook contact list.

Q. Okay.

11:21:51 And would I know this was going on?

A. No, you would not.

Q. All right. Let's go back one. Okay. One of the files you have listed here is called sys restore and you have that as system. What does sys restore do?

11:22:25 **A.** So there's a feature, a Windows feature that allows you to restore files if something goes wrong on your computer. So what Windows does is automatically take a copy of files on your computer and keeps a version. So if something goes wrong with your computer, you can go and 11:22:47 restore them from the restore program. And what this module does is it is deleting those copies so that if you wanted to restore files, there are no files there for you to restore.

Q. All right. And what about Win Defender? What is that folder?

11:23:09 **A.** Win Defender is an and antivirus program from Microsoft, and what the Win Defender module does is turns off the antivirus on your computer, the Windows Defender antivirus program on your computer, so that Windows, Microsoft Defender doesn't get a chance to detect the virus 11:23:27 on your computer.

Q. Does that mean that it wouldn't detect any virus on your computer because it's completely turned off?

A. Yes, that's correct.

Q. Okay. Let's take down Exhibit 1425. Thank you so much, Sue. 11:23:41

Let's now talk about the eBay fraud part of this. So for lack of a better term, you testified that you did an undercover operation related to the Bayrob Group's eBay fraud; is that right?

11:23:55 **A.** That's correct.

Q. And at a general level, can you please describe that undercover operation?

A. So what I did was I infected my computer with the Bayrob virus, and then I created a persona with an e-mail: 11:24:12 Address, user name, and an e-mail address, and I signed up for the fake auction that Bayrob was running, and I pretended I was a victim and then I -- the same procedure a victim would go through if they were buying a car, and I recorded all of that information. And part of that process: 11:24:35 Was that the Bayrob virus could intercept the information you would see when you went to eBay, so you could no longer trust the information that you were receiving back from eBay.

And one of the things that the Bayrob Trojan did was 11:24:53 it changed the help page on eBay and put in fake help information. And one of the things that it did was it put in a fake support chat auction. And so that if you were having difficulty with your fake auction, you could go and you could chat to the eBay support, which is really the Bayrob Group. 11:25:15

So what I did as part of my operation was I tried to engage the Bayrob Group in a conversation in that chat program to understand their capabilities.

Q. All right.

11:25:32 So let's just step back a little bit on that. So you did this undercover operation on one of your infected computers?

A. Yes.

Q. And it was infected with the Bayrob Trojan?

11:25:42 **A.** Yes.

Q. And your computer was infected with the Bayrob Trojan. What happened when you visited web pages on eBay?

A. You would not see the real content of all pages. So some pages, when you visited eBay, some pages you would see 11:26:02 would be the real content from eBay and some pages would be intercepted by the Bayrob virus on your computer. And instead of you seeing the real content that was being delivered from eBay, they would switch it out with their fake content, which was trying to sell their car.

11:26:20 So even though you were logged into eBay, you logged in with your user name and password, you could look around eBay and all the information you would see was the real content. When you went to the Bayrob auction, that auction did not exist on eBay, and it was being injected by the 11:26:43 Bayrob virus instead.

Q. What do you mean injected?

A. So when you -- when you visited a web page, you make a request to the, to eBay -- let's say you make a request to eBay and eBay gets your request and then it sends back down 11:26:57 the contents of the web page, the pictures and the text, the auctions, something like that, and sends it back down to your computer. And normally that's all that happens. You request, you make a request, the content gets delivered back to you.

11:27:12 But, what the eBay virus was doing was it was stopping that process. And when the page was delivered back from eBay before it was shown to the victim, the Bayrob virus was able to go in there and change what was seen on the web page and then show it to the victim.

11:27:28 To the victim -- to the victim, it appeared as if the information was really coming from eBay and it was a request they really sent to eBay, but in the background, unknown to the victim, the Bayrob virus was actually changing the content.

11:27:41 **Q.** Okay.

And you're using the word request. But, by request -- what are you referring to by request? If I was using eBay, what would it mean to make a request for eBay?

A. Well, if you went to your browser and you typed in 11:27:54 www.eBay.com, you're making a request to view eBay.com website.

Q. What if I click on one of the links on eBay for a particular car? Is that also a request for eBay?

A. Yes. Every time you want to get something from a 11:28:10 website like that, you click on a link. In the background, a request is sent to eBay and the content is sent back.

Q. Okay.

Let's take a look at Government's Exhibit 1431. I'm going to represent that this is an 80-page exhibit. We're 11:28:36 not going to look at all 80 pages. But, what does Exhibit 1431 represent?

A. Can I see this -- the second page?

Q. I'm going to hand you the whole thing.

A. And so these are the fake pages that eBay would -- 11:29:04 that Bayrob would show you instead of the content.

Q. So does this mean -- this is an 80-page exhibit, and I can bring it back to you if you'd like, but does this mean there are at least 80 blank pages?

A. So there was a -- for every stage in an auction on 11:29:30 eBay, if the Bayrob virus needed to change the content on that page, then it was a fake page stored on your computer that would allow them to change that content.

So, for example, when you want to look at the details of the car on eBay, you know, you see the picture of the 11:29:49 car, you see the price, all that type of information, there was a fake page on your computer that the Bayrob virus would deliver, instead of the real content from eBay.

And so, for example, if you wanted to research the seller, a lot of times before people buy they want to make 11:30:08 sure the seller is reputable, and so if you want to see if the seller's reputable you would go and check the seller's reputation on eBay. And the Bayrob virus had a fake page for that. So when you requested the seller's information, how many cars they sold, were they trustworthy, how many 11:30:26 transactions they've done in the last six months, the Bayrob virus would intercept your request and instead they would show you fake information so that the seller looks like he was really reputable when that was actually fake information.

11:30:38 **Q.** So let's look at Page 2 of this exhibit. There we go. And if we can zoom in on top. Okay.

So is this one of the fake pages that the Bayrob Group would inject on to eBay?

A. Yes.

11:31:03 **Q.** And on the right there, what does that -- where it says top rated seller, is this what you were referring to?

A. Yes.

So this is a replica of the real eBay page, but this is stored on the victim's computer. And this is shown to 11:31:24 the victim instead of the real page on eBay. And this is the template, and the template needs to be filled in with information about the auction that the victim is, you know, going to become, going to have their money come out of them in relation to.

11:31:42 So on the right-hand side, top-rated seller, you can see underneath that here that there's the percentage, seller, underscore name, percentage. And that is a marker to be changed to the seller name that the Bayrob Group decided to put in there when they go to show that page. 11:32:05 This is template to be filled out with information about the particular auction that the victim is going to see.

Q. So all the information between vintage signs, year make, model, sub model, that's all information to be filled in by the Bayrob Group?

11:32:24 **A.** Yes.

Q. And is that -- would that happen through an automated process?

A. Yes, it would. It was a separate request that was made to the command and control server, and the command and 11:32:35 control server would understand what car that particular victim was meant to be sold, and then they would send down that information. So they would send down the year, the make, the model, the sub model, the price, the seller name, the item number, all the things you see here and much more.

11:32:53 They would send that down separately. And then when the Bayrob virus was going to show this page to the victim, it would merge those two pieces of information together. It would take this page, and it would replace the percent, year percent with the year that it had -- had been received from 11:33:08 the command and control server.

Q. So it says here that this is a top rated seller with 100 percent positive feedback and 106 green stars, whatever that means. Is that accurate or is that information pre-plugged in by the Bayrob Group?

11:33:25 MR. GOLDBERG: Objection.

THE COURT: Overruled. You may answer that.

THE WITNESS: No, this is fake information.

THE COURT: I'm sorry, sir?

THE WITNESS: This is fake information.

11:33:34 **Q.** If we can turn to Page 5 of the same exhibit, what is Page 5 of this exhibit?

A. So Page 5 is a screen -- is a -- it's a template to replace Carfax. And when a victim --

Q. Sorry. Can I ask what is Carfax?

11:34:05 **A.** Carfax is a website you can go to, to get information about a car. And if you're going to buy a car, you go to Carfax and you can put in the Vehicle Identification Number into Carfax and it will tell you if the car has been in any crashes, how many owners it has had, information like that, 11:34:24 reputation service for buying and selling cars.

Q. So what does this page do?

A. So the Bayrob virus was not just able to intercept requests to eBay.com, it was also able to intercept requests for Carfax.com and so whether you -- when a victim would be 11:34:47 doing the research about whether they should buy this car on eBay, generally it looked like a very good deal and they would want to know if the car was in good condition, if it ever been crashed, things like that.

So what they would do is they would go to Carfax and 11:35:02 request the information about the car. And instead of seeing the real Carfax page, they would see this fake page instead and just the fake page would always say it was in great condition, it had one owner, and that it was a legitimate sale.

11:35:19 So this would give the victim confidence they could proceed with the sale.

Q. All right.

If we could look at Page 16 of this exhibit. So what are we seeing on this page?

11:35:43 **A.** This is a fake, "Ask a Question" page. So if the victim wanted to ask a question about the fake auction, they could come here and they could ask a question, you know, is the car in good condition, any questions that they would have, you normally would have if you're trying to buy a car.

11:36:02 And you can see here the same percentages surrounding key words like seller name. So this is information that would be filled in from the Bayrob virus before this page was shown to the victim. And if the victim asked the question here, the question would not go to the real seller. 11:36:22 There was no real seller. The question would go to the Bayrob instead.

Q. And specifically, would it go to the command and control server?

A. Yes.

11:36:32 **Q.** If we could take a look at Page 21. What is -- not there. What does Page 21 show?

A. Page 21 shows the fake feedback page for the seller. I'm showing the seller is in good standing. You can see here it shows that they have the last six months, they had 11:36:59 21 positive engagements on eBay, and over the past 12 months they had 44 positive engagements, and they had zero negative engagements, and you can see they got a five-star rating from some past buyers. And at the bottom, you can see comments that past buyers have left.

11:37:21 But again, this is all fake information. You can see the seller name here is inside percentage, percentage signs again. So this is the template that will be filled out by the eBay virus. And it will be shown to the victim. If the victim tries to understand that the seller is a reputable seller. 11:37:45

Q. Those comments at the bottom about the seller, what's the source of those comments?

A. They were -- they were from the Bayrob Group.

Q. Okay. They're not from satisfied customers?

11:38:02 **A.** No.

MR. O'SHEA: Objection to the form.

THE COURT: Sustained.

Q. How do you know who they're from?

A. This information -- this template was sent from the command and control server. 11:38:14

Q. Let's turn to Page 42 S what is Page 42 here?

A. This is a page to be shown to users, to victims, to steal their credit card information.

Q. And how would that work?

11:38:53 **A.** The Bayrob virus was able to decide if it should steal your information or not. And if it decided to steal your information, it could show you this page and solicit your information that way.

Q. If we could look at Page 50, please. What does this page show? 11:39:28

A. So this shows the information about how to make a purchase on eBay. This was a page delivered by the Bayrob virus as well.

Q. Okay.

11:39:42 And at the bottom, there's a question. What is that question?

A. It says, "How does eBay Buyer Protection through an eBay agent work?"

Q. And let's turn to the next page, Page 51, and let's go 11:40:02 to the last question and answer there. What does eBay buyer protection to an eBay agent cover?

And basically what is this?

A. This is information to convince the victim how they should proceed with their purchase on eBay.

11:40:23 **Q.** Okay.

And was there -- without going through all 80 pages, was there a lot of information in these pages about how to make a purchase on eBay?

A. Yes. The Bayrob --

11:40:38 MR. O'SHEA: Objection.

THE COURT: Overruled. Go ahead.

THE WITNESS: The Bayrob virus, the goal of the Bayrob virus was to make --

MR. GOLDBERG: Objection.

11:40:50 THE COURT: Sustained. Sustained.

BY MR. LEVINE:

Q. What did the, these eBay pages direct the buyer to do with respect to large payments?

A. They directed the victims to use an eBay agent.

11:41:11 **Q.** And how -- more specifically, what steps would it advise them to take?

A. So they would advise the user to get protection when they were buying the car and to use an eBay option to protect their purchase. And the way they could protect 11:41:34 their purchase was by using an eBay agent and the benefit of using an eBay agent, which is what the information here is showing, is that your purchase was protected and that you could inspect the car before your money will be taken.

Q. All right.

11:41:50 Let's look at Page 61. And if you could, Page 60. Is this a description of the eBay agent account program?

A. Yes, it is.

Q. Okay.

And if you could read the line in bold. First of all, 11:42:26 did you bold that line or was that bold already in the page?

A. No, this is to information that came from, directly from the command and control server. I didn't bold this.

Q. Okay.

If you could just read that first paragraph under 11:42:39 overview there.

A. "The eBay Motors Vehicle Protection -- Vehicle Purchase Protection Program provides protection of up to $50,000 against certain losses associated with some types of fraud. You are automatically enrolled in the program at no 11:42:55 charge when you complete the purchase of an eligible vehicle on eBay motor site. If the seller offers payment to an eBay agent account, we suggest you use this as it will make a refund easier should that be the case. Your funds will be in eBay's custody and will not be released to the seller 11:43:15 until you have received and approved the vehicle you are purchasing."

Q. Okay.

And again, we're not going to read them all but are there many pages that are part of this 80-page exhibit that 11:43:28 discuss this buyer protection program?

A. Yes, there are.

Q. Okay.

Now you said these pages were actually stored on the infected computer?

11:43:41 **A.** Yes, that's correct.

Q. Would a normal user be able to find them on their computer?

A. No.

MR. GOLDBERG: Objection.

11:43:49 THE COURT: Overruled. It will stand.

Q. How were you able to find them?

A. These files are encoded on the computer so they're not easy for a normal user to see. And I was able to find those files and decode them so that I could see the content.

11:44:08 **Q.** Okay.

So now I want to move to your undercover operation. And I'd like to look at what has been previously marked as Exhibit 1432. And what is Government's Exhibit 1432?

A. This is a screenshot I took of an auction that I participated in. 11:44:30

Q. Okay.

Is this any option on eBay or is this one from the Bayrob Group?

A. This is one from the Bayrob Group.

11:44:38 **Q.** All right. Looking at this exhibit, can you tell us which of the content here is injected by the Bayrob Group and which is from eBay?

A. All of the content on this page is from the Bayrob Group.

11:44:52 **Q.** Okay.

So the top rated seller information, that is from the Bayrob Group?

A. Yes. So this content is a merge of the template we saw earlier and the specific information about this auction that was sent out from the command and control server. So 11:45:13

the year, the model, the make, the price, the seller, all of this information was received from the command and control server and it was merged into the template we saw earlier, and then this page was shown to the user instead of the real eBay page. 11:45:32

Q. And if you could read the eBay agent protection that's listed there, I would appreciate that.

A. "For large transactions, we recommend choosing our new payment option, which allows you to make the transfer up to an eBay agent account. 11:45:47 This account will act as an escrow account until the item is received and inspected by the buyer. The money will not be sent to the seller until the buyer confirms that the item is as advertised in this auction."

Q. Okay. 11:46:02

Now, in the upper right-hand side, is there a button called Live Help?

A. Yes, there is.

Q. And what is that button?

A. Live Help directs to you a chat window where you can chat with the eBay help, which is not actually eBay help; it's actually the Bayrob Group. 11:46:13

Q. Okay.

And did you click on that Live Chat button?

A. Yes, I did. 11:46:31

Q. Let's look at Government's Exhibit 1433.

So when you clicked on that Live Help button, is that what you saw?

A. Yes, it is.

11:46:56 **Q.** And this is how you saw it in one of your infected computers?

A. Yes.

Q. Is it a screenshot you took?

A. Yes, it is.

11:47:11 **Q.** Now as part of your undercover operation, did you fill out this form based on a fake identity and hit send?

A. Yes, I did.

Q. And did you use some type of screen reporting program to record part of your chat on eBay?

11:47:25 **A.** Yes, I did.

Q. And does that program make a fair and accurate reporting of your chat on eBay?

A. Yes, it does.

Q. And did you provide two video files to the Government 11:47:35 made by that recording program?

A. Yes, I did.

Q. Now in the video files you provided to the Government did you increase the speed of the videos a little bit to make them more tolerable to watch?

11:47:49 **A.** Yes, I did.

Q. Did you make any other changes to the videos?

A. No, I did not.

Q. Okay.

Now in the video files you provided, is your screen name Carmel Brown 2012? 11:47:59

A. Yes, it is.

Q. And is the screen name of the purported eBay agent you're chatting with Sarah A?

A. Yes, it is.

11:48:11 **Q.** Okay.

MR. LEVINE: So, your Honor, these two video files have been provided to the Defense as part of discovery. What I'd like to do is play one video and then the other. And I would like to ask, especially for those who might not be able to read as quickly, I'd like to ask 11:48:27 Mr. Omurchu if he would be willing to narrate the chat as it occurred.

THE COURT: Certainly.

MR. LEVINE: Thank you, your Honor.

11:48:43 MR. O'SHEA: Which one first, Brian?

MR. LEVINE: First, we'll start with 1344.

THE WITNESS: So I have -- I don't -- I don't need to have someone inspect the vehicle before I buy it. So I'm talking to the eBay help and trying to ask questions -- 11:49:08

Q. Stop for a moment. Could you pause it for a moment and start it over? Is it possible to zoom in on 24 mode on the chat window or not?

MS. CHANDLER: No.

11:49:31 **Q.** Okay.

Before we start narrating, could you describe what we're seeing here on this --

A. Oh, sure.

Q. -- screen?

11:49:38 **A.** So when you click on the Live Help link and you log in or you enter your information that you showed on the previous slide, you're brought to this page and this is a web page but it's a chat web page that allows me to chat with supposedly eBay help.

11:49:54 And you can see in the URL bar that it's --- eBay.com is LiveHelp.corp.eBay.com is the website I'm on. So it looks like I'm communicating with eBay even though I'm not. And this is me, Carmel Brown 2012, and I'm asking some questions. And Sarah A is pretending to be the eBay help, 11:50:22 and she is answering my questions.

Q. And before we start playing it, can you just read what's already on the screen in terms of your conversation?

A. Sure.

I said, "I haven't bought a car before on eBay before. 11:50:34 So sorry if my questions are obvious." And so I see there is an agent option. And then Sarah A replied, "Thank you for contacting eBay. Please hold while I check the auction details for the item you provided. You can pay to an eBay agent. That way you will not be sending money directly to 11:50:53 the seller. You can you will not be sending money to a seller but to one of our agents. We would then instruct the seller to ship the vehicle. When you receive it, you will have three days to inspect it at your home.

"Be assured your money is safe with us, and we will 11:51:07 not release the funds until you approve the vehicle. We cover title and registration issues, misrepresentation, and damage."

Q. Okay.

So we're going to start and if it's going too fast for 11:51:21 you to narrate exactly, you can tell us the thrust of what the -- what you were saying in each line and what the response was.

A. Okay.

Q. Let's try playing it now.

11:51:38 **A.** Okay. So I don't need to have someone inspect the vehicle before I buy it. This is me asking the question.

And Sarah A comes back. And if there's something wrong with the car, do I need to -- do I need to pay to ship it back? And that could be a lot of money. My question to 11:51:59 eBay help.

And then Sarah A comes back and says, "No. The return fee is already paid." And I say okay great. And so I say, "Okay. So I just need to research on the seller? And you see the car seems to be very good price. So I'm a little 11:52:37 suspicious. Seems too good to be true." And Sarah A has come back and said, "After you send the funds to our agent, we will notice the seller to ship the car to you for inspection. You will have the chance to inspect it for three days. If you accept it, we will forward the funds to 11:52:51 the seller. If not, we will send you a full refund."

And then Sarah replies and says, "And your item checks out. The auction is legitimate. This seller has a very good rating."

Q. Continuing with Sarah.

11:53:15 **A.** "You can proceed with trust this purchase is fully refundable up to $50,000 through the eBay Bank Protection Program."

And then I said, "Okay. That sounds good. Do you know how long it takes to ship a car? Does eBay track that 11:53:31 or do I need to track it with the seller? You hold the money no matter how long it takes. And sorry for so many questions. I think I will buy it. So I want as much information as possible. And if anything goes wrong, who do I contact? Can I just do this chat again or -- and okay. 11:53:57 Thanks."

And Sarah came back and said, "We will hold the money no matter how long it takes to ship the car. You will receive complete documentation and complete instructions, along with the car. eBay will track the shipment. You will 11:54:12 just receive it at your door."

And I say, "Okay. Thank you. You've been a great help, Sarah." And Sarah says, "Usually the shipping process takes four to five business days. And anyway, if you decide to make the purchase, please come back on live chat so I can 11:54:29 guide you through the process. And also I will give you extra information about the security measures that will apply but first, you need to make the purchase."

And then I say, "Okay. Thank you. Do I need to use a reference number for this chat?"

11:54:44 And Sarah replies and says, "No. We keep records of all chats. Just come here and we will know about you and you're welcome."

And then I say, "Thank you. Bye."

And Sarah says, "If you want to make the purchase now, 11:55:08 you can remain here on this chat." So she is trying to convince me to make the purchase right now. And I said, "Okay. I'm going to think about it."

She says, "Before I let you go, is there anything else I can assist you with?" And I said, "No, you've been a 11:55:21 great help. One last thing. And what is the fee for using the eBay agent? And is it a percentage or just a one-time fee?"

I was trying to think of any questions I could ask to engage the person: And Sarah A comes back and says, "It's a 11:56:00 percentage and equal to 0.75. In your case, it will be $72.75." And I said, "Okay. Not so much. Seems better to use the agent. Thanks. Talk to you soon."

Q. So --

THE COURT: Is that it for this one?

11:56:29 MR. LEVINE: For this video, yes.

THE COURT: All right. We're going to take our luncheon recess.

Folks, remember the admonition. Do not form any opinion. Do not talk about the case. Please be downstairs 11:56:38 at 1:00. We will call for you as a group and bring you up.

Have a good lunch.

(Thereupon, a luncheon recess was had.)

WEDNESDAY SESSION, MARCH 27, 2019, AT 1:00 P.M.

THE COURT: You may continue.

MR. LEVINE: Thank you, your Honor.

BY MR. LEVINE:

13:08:39 **Q.** Mr. Omurchu, when we broke, you were looking at this video of an eBay live chat. And who were you -- who was Sarah A that you were chatting with?

A. Sarah A was the name that the eBay help agent was using.

13:09:00 **Q.** Okay. And was it a person from eBay or was it a person from the Bayrob Group?

A. It was a person from --

MR. O'SHEA: Objection.

THE COURT: Sustained.

13:09:10 **Q.** Do you know whether it was a person from eBay or a person from the Bayrob Group?

MR. O'SHEA: Objection.

THE COURT: Sustained.

Q. When you had this chat, were you on the eBay website?

13:09:23 **A.** No.

Q. Where was this chat?

THE COURT: Did you say no, sir?

THE WITNESS: Yes.

Q. Where was this chat being generated from?

13:09:32 **A.** This was being generated from a command and control server controlled by the Bayrob Group.

Q. Okay.

And this chat window we see here, is that some kind of chat program?

13:09:44 **A.** Yes, it is.

Q. And is that a chat program that is from eBay or was it from the command and control server?

A. It was from the command and control server.

Q. If we could bring down this video and move to the second video that was just up, please. 13:10:02

THE COURT: Please identify the number.

MR. LEVINE: The next is Exhibit 1435. And before you play it --

Q. Can you tell us what is the context for the second video? 13:10:25

A. So the second video is at the end of the first video. I hadn't bought the car yet. And the second video is where I go back onto the eBay chat and I proceed to buy the car.

Q. Okay. So this is a continuation of the same transaction that you discussed in Exhibit 1434? 13:10:44

A. Yes.

Q. Okay.

So now I'm going to ask you -- we'll play this video. And if you could narrate it as you did before, that would be very helpful. 13:10:55

A. So I clicked on the live button and the chat window has opened up. And I'm going to put in my information here, and my user name, and the item number that I'm interested in buying, which is for the 1970 Chevrolet shown in the 13:11:17 background. This is the item number for that car that's on the -- showing in the page in the back.

Q. Is that number a number that the Bayrob Group created?

MR. O'SHEA: Objection.

THE WITNESS: Yes.

13:11:36 THE COURT: Sustained.

MR. LEVINE: Can we pause there, please?

Q. Where did that number -- where did you get that number from?

A. From the command and control server.

13:11:44 THE COURT: I'm sorry, sir?

THE WITNESS: From the command and control server.

Q. Well, was it -- let's step back. Was it on the page that we're seeing in the background on the screenshot?

13:11:54 **A.** Yes.

Q. And where was that page coming from?

A. From the command and control server.

Q. Okay.

And so why were you seeing it on your computer?

13:12:04 **A.** Because I was -- the virus I had on my computer was trying to encourage me to buy this car. So when I went to visit the link that I had received from the Bayrob Group, I was brought to this page, with this Item Number at the top.

Q. Okay. Let's continue with the video.

13:12:33 **A.** So Sarah A is back in the chat program, says welcome back, and I say, "Hey, yes. I have another question. Can I pay with a credit card? The page, on the page it says bank transfer. I have never done one of those before. Is credit card also accepted -- acceptable?"

13:13:14 **Q.** And is this you waiting Sarah A's response?

A. Yes. And I wanted to understand if they were going to push me to use the eBay agent or if I could do the transaction some other way. And also wanted to engage the help person in the conversation. I understood how the 13:13:40 auction worked at this point. So I knew exactly what I needed to do, but I wanted to engage the help desk in conversation.

And Sarah A comes back and says, "No, you will have to go to your bank in person and make a bank wire transfer to 13:13:53 our agent." And I say okay. And I say I'm ready to buy it now.

Sarah A comes back and says, "It's like any other regular bank wire transfer." And then I say okay. And I say do I -- do I need to say I want to use the eBay agent 13:14:20 option before I buy it or after? What do I do next?

And Sarah A comes back and says, "Still there?" And I said yes. And then I said I want to buy the car, but I want to know how to select the eBay agent option.

And Sarah A comes back and says, "First, you need to 13:15:35 win the auction through the Buy It Now, through Buy It Now, then you have to choose the eBay agent payment option. Then you will need to request an agent. So now I go back to the eBay page to see can I click the Buy It Now button. And I have to log back in first. So I log back into eBay. And I 13:16:02 click the Buy It Now button, and then --

Q. Pause for one second. Are you actually on the website here or are you on pages sent to you by the Bayrob Group?

MR. O'SHEA: Objection.

THE COURT: Overruled. You may answer that.

13:16:22 THE WITNESS: The URL says offer.com. So i appears like I'm on the real eBay website but this page I see here is a fake page that the eBay -- that the Bayrob Trojan has injected and is showing that instead.

BY MR. LEVINE:

13:16:40 **Q.** Okay. Let's unpause it.

A. And I click it to the Commit to Buy button, and I go back to the live chat. And in the background, you can see you've purchased -- you've committed to buy the car now. And now, I can see the option to use an eBay agent. And I 13:17:05 go back and I say okay, now I see that option. And I choose to pay with an eBay agent option and I fill in the information, the name, and the fictitious address. And Sarah A comes back and says now enter details.

So that's what I'm doing here. And I enter in my 13:17:55 details. Sarah comes back and says, "Are you still there?" I say, "Yes. I entered the details."

So it's telling me to pay $9,772.75, and -- but I still don't see where I'm to pay that information. And Sarah comes back and says, "When do you think you'll be able 13:18:27 to make the bank wire transfer? I need to know these details in order to make the best choice in assigning an agent."

So I come back and say I'll be able to go to the bank before work tomorrow. And I said I was going to go to the 13:19:01 bank tomorrow so that I could have the transaction completed as quickly as possible. And I'm waiting for Sarah A to come back and tell me what I need to do next.

And then Sarah A comes back and says, "Okay. I'm assigning an agent right now. Please hold." And then I 13:20:17 respond saying, "Okay. I'll wait." And Sarah A comes back and says, "An agent has been assigned to your sign. Please refresh the page to see the details."

So I go to the item page, and there's no details yet. So I need to refresh the page. So I refresh the page.

13:20:35 **Q.** And you refresh the page. How do you --

A. By hitting the refresh button. And now that I've refreshed the page. I see the agent details in the window behind.

And Sarah has written quite a bit in the meantime. 13:20:53 And an agent has been assigned to your transaction. And then information about how to proceed, and protection against authorized account access. And because you've chosen this payment method, I want to give you details on some of the security measures that would apply to protect 13:21:10 the community against unauthorized account has started, noting which computer members use for protection. If you attempt to sign in from an unknown commuter, for example, from a library or hotel, eBay may temporarily block your account access. Be advised that when choosing the eBay 13:21:27 agent option, this auction will be restricted to this computer only. This auction will not be accessible from other computers. This is for your security. We want to make sure nobody is able to hijack your account. Also please do not access your account from another computer as 13:21:39 we may block your access.

Q. Can you pause for a second?

If you were to access your eBay account from another computer, will you be able to see this auction at all?

A. No. You can only see this auction on the computer 13:21:50 that is infected.

Q. Okay. Please continue.

A. And then I say, "Okay. I see the details now. I will bring them to the bank tomorrow, and I'm sure they will know now to take care of this."

13:22:04 **Q.** Can we pause for a second?

So if you look to the left there behind the chat window, what are we seeing?

A. So we're seeing the eBay agent information that has been provided to me where I need to make my payment, and the 13:22:19 beneficiary name is Crystal Y. Hart, and I'm given the bank name which is Wells Fargo, and the routing number, and the account number, and the bank address, and the beneficiary address. And this is to -- these are the details that I would need to go to the bank and make the wire transfer.

13:22:39 **Q.** Now, that page that we see those details on, is that on actual eBay or is that on a page injected by the Bayrob Group?

MR. O'SHEA: Objection.

THE COURT: Sustained.

13:22:50 MR. O'SHEA: May we approach?

Q. Where is that -- where are --

THE COURT: One moment.

MR. O'SHEA: Can we approach real quick on this?

13:22:57 THE COURT: You may.

(The following proceedings were held at side bar:)

MR. O'SHEA: The basis of my ongoing objection is that I don't have problem saying it came from the command and control server, but for him to say it's the Bayrob 13:23:25 Group, there's not enough foundation for that yet and that's a jury question.

MR. LEVINE: Thank you, your Honor.

Liam has -- the witness has named the group on the malware that does this, including the command and control 13:23:47 server, the Bayrob Group. He came up with that name. He's not referring to any individual person. He's referring to the group and malware that he has identified by that name itself.

THE COURT: I agree with you. However, I need 13:24:02 you to preface it -- in other words, you need to do the foundation better when you ask each of those questions.

MR. LEVINE: Okay.

THE COURT: You follow me? And I know you're going to say, "But, Judge, I've already done it." So I 13:24:25 don't have any problem allowing it with the foundation question. And I want you to do it every time you ask this question.

MR. LEVINE: I will do that.

THE COURT: Okay. And I understand that -- 13:24:37 that your general objection, I understand it. But, I want the foundation so that the jurors are reminded of how, in fact, it's -- it's coming from quote, unquote, the Bayrob Group.

MR. LEVINE: Okay. Very good. Thank you.

13:24:57 MR. BROWN: Thank you.

(Proceedings resumed within the hearing of the jury:)

BY MR. LEVINE:

Q. So the eBay agent account information there, is that coming from the virus or is it coming from eBay?

13:25:20 **A.** It's coming from the virus.

Q. Okay. Let us --

A. I don't see anything on my screen at the moment.

THE COURT: I'm sorry?

THE WITNESS: I said I don't see anything on

13:25:29 my screen at the moment.

THE COURT: That's not good.

THE WITNESS: I can see it now.

THE COURT: Thank you.

BY MR. LEVINE:

13:25:45 **Q.** Okay.

So you testified that this eBay account information is coming from the buyer, correct?

A. Yes.

Q. And this is on the computer that you infected?

13:25:55 **A.** Yes.

Q. What virus did you infect your computer with?

A. Bayrob.

Q. Okay. Let's continue the video, please.

A. I said, "Okay. I see the details now. I'll bring 13:26:18 them to the bank tomorrow and I'm sure they will know how to take care of everything." And Sarah A replies and says, "Just tell them you want to make a regular bank wire transfer. Provide them with our agent details as the receiver then fax us the bank receipts at this number. 13:26:34 866-554-2685 so we can process your payment faster. I think everything is set. Please fax us the bank receipts tomorrow."

And I replied and said, "Okay. Thanks for all your help. Then I'm highlighting the agent's details that I have 13:27:01 been given."

Q. Okay. All right. Thank you.

Do many commercial websites where you can buy products have a live chat feature like that?

A. Yes, a lot do.

13:27:14 **Q.** But, to be clear, this one was not eBay's live chat?

A. No.

Q. All right.

Let's bring up what's been previously marked as Government's Exhibit 1436. What is Government's Exhibit 13:27:38 1436?

A. This is a log of chats that victims had with their eBay Live Help service.

Q. Okay. Where did you identify this chat log?

A. The chat log was stored on the command and control server. 13:28:01

Q. Okay. And were there many chat logs with victims stored in the command and control server?

A. Yes, there were.

Q. And have we redacted out the victim lines in this chat? 13:28:15

A. Yes.

Q. Other than the redaction of the victim lines, is this how that chat log appeared to you on the command and control server?

A. Yes, it is. 13:28:25

Q. Now, looking at this page, how are these chats organized on the command and control server?

A. They were grouped together, showing they -- the victim as you, and the agent, agent name in this case, Allister S -- 13:28:55

Q. Before you go into reading part of this --

A. Okay.

Q. -- were the chat logs with victims all in one file or separate files for each victim? How is it organized on the command and control server? 13:29:08

A. There were multiple chat logs. I think each log contained multiple conversations.

Q. Okay.

So now looking at the first page, can you explain what 13:29:21 those fields are at the top of the page?

A. Yes. So the op -- op is short for operator. That's the eBay help person that you are chatting with.

Q. And your chat, who is that?

A. Sarah A.

13:29:35 **Q.** Sarah A. Okay.

A. Here it's Allister S.

Q. Now can we save --

A. And then underneath that is the time, and it tells you the time that the chat happened at.

13:29:49 **Q.** So what is -- what is that time? Doesn't look like a time.

A. It's a -- it's a number that the computer can convert into a regular time, like date and time.

Q. Okay.

13:30:02 **A.** ID is the name of the victim -- the use -- the identifier that the victim was using, and this is called zoneA1979.

Q. Is that like a user name?

A. Yes, a user name. And e-mail is the e-mail of the 13:30:19 victim, calzone420@yahoo.com. And name is a person's name;

in this case, Cal Easton. And IP is the address of the infected computer that Cal Easton is using?

Q. By address, you mean IP address?

A. Yes, IP address.

13:30:39 And the host is another way to describe the IP address. The location is the next field, and then the item.

Q. Can you hold for a second there.

So the host lists -- appears to list IP address, and it says PAComcast.net. What does that mean?

13:31:02 **A.** That means this person is using Comcast for their home Internet connection.

Q. Does the PA suggest anything?

A. I'm -- I don't know.

Q. Okay. What about -- at location, there's no 13:31:14 information?

A. Yes, that's right.

Q. Okay.

A. And then there's an item number after that, and then after that, there's the browser that the victim was using. 13:31:25 In this case, they're using MSIE, which is Internet Explorer, and the version that they're using is 8.0.

Q. Okay. Can we back up?

And so I think we saw that -- did the eBay pages used by the Bayrob Group also provide a page where the eBay user 13:31:46 could contact the seller of the vehicle with questions?

A. Yes.

Q. And did the Bayrob Group also collect a catalog those questions from users to the seller?

A. Yes, they did.

13:31:56 **Q.** All right.

So if we could bring up Page 2 of what has been marked as Government's Exhibit 1437.

THE COURT: 1437?

MR. LEVINE: 1437, yes. Oh, 14 -- yes, this
13:32:15 is right. We're on to a new exhibit.

Q. So what are we seeing here in Exhibit 1437?

A. This is a log of questions that victims asked when they're infected with the Bayrob Trojan.

Q. Okay. And where did you find this?

13:32:39 **A.** I found this on the command and control server.

Q. And was this information -- how would this information get on the command and control server?

A. It was sent from infected machines to the command and control server.

13:32:52 **Q.** And is that an automatic processor? Does the victim have to send it?

A. So when the victim is viewing a fake auction, they can click on "Ask, et cetera" link, and when they click on the, "Ask, et cetera" link, they can type in the question. And
13:33:07 whether they hit send, instead of that question going to a

legitimate seller, it's going to the Bayrob Group instead and being sent to the Bayrob command and control server.

Q. Okay. So if we could zoom in on the first line.

So what are we -- if you could go through and explain 13:33:32 what each of these fields are.

A. So the e-mail is the e-mail of the victim, mega@laplaza.org. And the LICI is the identifier of the operator and the car. And it's an auction identifier, and the date is the date that the question was asked. And the 13:33:54 IP address is the IP address of the person's computer, and the host is the same thing. It's the address of the victim's computer. And then after that, there's a question. This is a question that the victim or potential victim, certainly the person who's infected at the moment, asked. 13:34:14 And they asked are the photos current, the photos of the car, are they current or are they shortly after the restoration? How's the car being stored inside since the restoration? Was the engine, transmission, and suspension rebuilt during the restoration?

13:34:32 **Q.** Okay. Can we take this down now? I want to change subjects now and talk about where the money went.

When eBay victims thought they were wiring the money to an eBay escrow agent, as we just saw in the video, where were they actually wiring their money to?

13:34:50 **A.** They were wiring their money to what are called money mules.

Q. Okay. And what is a money mule?

A. A money mule is a person who will receive money and then send it on to another location and act as a middle man. 13:35:06 And generally they take a commission for doing that. And sometimes they understand the implications of what they're doing. Sometimes they don't.

MR. O'SHEA: Objection.

THE COURT: Sustained.

13:35:22 MR. LEVINE: Should I have the witness repeat the answer minus the last part or what portion?

THE COURT: I'm going to strike the whole answer and you can start over if you'd like.

BY MR. LEVINE:

13:35:35 **Q.** Okay.

Without getting into the mental state of a money mule, let me ask you again what is a money mule?

A. A money mule is a middle man who takes money and transfers it somewhere else and generally takes a commission 13:35:48 for doing that.

Q. Okay.

And how did the Bayrob Group find people to work as money mule?

A. They recruited them from the web, via advertisements 13:35:58 or e-mails.

Q. Okay.

Let's bring up what's been previously marked as Government's Exhibit 1438. And if we could zoom in on that page itself. What is Government's Exhibit 1438?

13:36:22 **A.** This is a -- an advertisement to -- advertisement for a stay at home -- this is a screenshot I took of an advertisement to work from home.

Q. Okay.

And is it -- so where did you obtain this screenshot?

13:36:44 **A.** I obtained this screenshot from traffic from my infected machine.

Q. So explain what you mean by that.

A. So my infected machine was being used as a proxy where the Bayrob Group were connecting through my machine and they 13:36:59 were connecting out to the other sites to run their operation. And when they did that, they connected to this website and I was able to see that as they -- as the content passed through my machine.

Q. So, in other words, was -- was this an actual website 13:37:17 of on the Internet at some point?

A. Yes, it was.

Q. And what did you see over your machine related to that website out of the Internet?

A. Well, I saw what you see on the screen here. I saw an 13:37:34 advertisement and I saw the Bayrob Group accessing that page.

Q. Okay.

So the Bayrob Group was accessing this page on the web, but through your infected machine?

13:37:44 MR. O'SHEA: Objection.

THE WITNESS: Yes.

THE COURT: Sustained. Form of the question.

BY MR. LEVINE:

Q. Can you explain -- could you elaborate on how -- how you were able to see this page? 13:37:53

A. So they were connecting through my infected machine, and there was acting as a proxy so I could see all of the information that was passing through my machine that the Bayrob Group thought they were doing. And one of the activities they were doing was they visited this web page. 13:38:09 And when they did, that I was able to see that.

Q. Okay.

Could you see -- if the Bayrob Group was using your infected machine as a proxy, could you see everything they were doing on your infected machine? 13:38:22

MR. O'SHEA: Objection.

THE COURT: Overruled.

THE WITNESS: I could see everything but some of it was encrypted or where I wouldn't be able to determine what was happening in some of the traffic. 13:38:36

Q. Okay. And we'll talk about encryption a little later.

So let's look at the second page of this exhibit. What is this second page of Exhibit 1438 show?

A. This shows access -- it shows who accessed the host, 13:39:17 variousopinion.net, which is the website we saw on the previous screenshot. It's a log of who accessed that page at what time.

Q. Okay. And where did you obtain this?

A. The -- I obtained this from the website 13:39:34 variousopinion.net.

Q. It was on the website itself?

A. It was on the website itself.

Q. And it's a log showing what?

A. It's showing -- well, the name of the file is 13:39:48 click.txt, and it's showing information about who clicked on a link that pointed to variousopinion.net.

Q. Okay.

And is this information that would have been available to the Bayrob Group?

13:40:03 **A.** Yes.

MR. GOLDBERG: Objection. May we approach?

THE COURT: You may. And, Shirle.

(Discussion held off the record.)

(The following proceedings were held at side bar:)

13:42:27 MR. GOLDBERG: Just for the record, your Honor, I've objected to Pages 2 through 32, Exhibit -- Government's Exhibit 1438. My understanding was that Page 1 was an ad for work at home that did show up on the monitor traffic. What's on the rest of the pages is metadata from access to 13:42:59 that ad from elsewhere on the Internet, having nothing to do with Bayrob or the command and control server.

So to the extent that the jury's going to see all these click throughs to that ad having nothing to do with this case, I object to that being shown to the jury.

13:43:15 THE COURT: Do you agree that those pages have nothing to do --

MR. LEVINE: I disagree.

THE COURT: -- with Bayrob?

MR. LEVINE: No.

13:43:25 THE COURT: Well, let's ask him the question.

MR. LEVINE: I will clarify it on the record. It's a log that everybody who clicked on that ad with the Bayrob Group placed. So I would --

THE COURT: Let's get it clarified.

13:43:39 (Proceedings resumed within the hearing of the jury:)

BY MR. LEVINE:

Q. So to clarify the second page, is this the beginning of a log?

THE JURY: The jury can't see.

13:44:02 THE COURT: I'm sorry?

THE JURY: The jury can't see.

THE COURT: Nothing on the screen? We're going to get this worked out. Good?

THE JURY: Yes.

13:44:17 MR. LEVINE: Okay. Sorry about that.

Q. So on the first page of this exhibit we saw an advertisement to work at home for $7500 a month. What is the second page reflecting?

A. The second page is a log that was found on that website. 13:44:33

Q. It's a log of what?

A. Of access to that website.

Q. So is this a log of everybody who visited that website?

13:44:42 **A.** Yes.

Q. Okay. No further questions on this exhibit. So we can take this down. Okay.

Now, did the Bayrob Group also pretend to be search engine companies hiring wire transfer agents?

13:45:06 MR. O'SHEA: Objection.

THE COURT: I'm going to sustain it. Rephrase that.

BY MR. LEVINE:

Q. Did the Bayrob Group have another way or what other ways did the Bayrob Group hire wire transfer agents? 13:45:17

A. They had many different ways, but one way was to pretend, was to advertise wire transfer services as if they were from the legitimate companies.

Q. Like what legitimate companies?

13:45:38 **A.** Yahoo, for example.

Q. Okay.

If we could bring up Government's Exhibit 1439, please. And if we could zoom in on the contents. What is Government's Exhibit 1439?

13:46:02 **A.** It is a document showing an agreement to transfer money, and it purports to be from Yahoo transfers.

Q. And where did you find Government's Exhibit 1439?

A. I found this transfer between two members of the Bayrob Group.

13:46:28 **Q.** Over your infected computer?

A. Over my infected computer.

Q. Okay.

And who is this agreement supposed to be for? It's --

MR. GOLDBERG: Objection.

13:46:41 THE COURT: Overruled.

THE WITNESS: This agreement.

THE COURT: Can you answer that?

THE WITNESS: Yeah, this agreement is meant to be for people who have applied to be transfer -- to transfer

13:46:53 funds from one of the advertisements that the Bayrob Group put up.

Q. Okay.

On the second page of this, is this another agreement that you saw transferred over your computer?

13:47:21 **A.** Yes.

Q. The third page. What is the third page of Government's Exhibit 1439?

A. This is the content that could be added to an e-mail about how to recruit people to do the Yahoo transfers.

13:47:51 **Q.** Can you read it?

A. Sure. The subject is your Yahoo transfers contract.

And then, "Dear, dot, dot, dot. You need to fill in the name of the person you're sending it to there. In order to complete your application, please fill and sign the 13:48:05 attached document and e-mail it back to me or fax it at 1-866-929-3886. If you have any questions, please e-mail me back or contact me through Yahoo Messenger or if you are using a different IM, instant messenger software, like Skype, AIM, MSN, Google, please let me know what your user 13:48:29 name is there so I can add you on my list. Regards, Kelemen Donath."

Q. So the sender of this e-mail letter, this template purports to be someone by the name of Kelemen Donath?

A. Yes.

13:48:45 **Q.** And a couple of those words, what is A-I-M, AIM?

A. It's a chat program.

Q. What does it stand for?

A. AOL Instant Messenger.

Q. What about MSN?

13:48:55 **A.** It's Microsoft. It's another chat program from Microsoft.

Q. Okay.

Did the Bayrob Group also collect and maintain a log of questions they received from potential money mules?

13:49:13 **A.** Yes.

Q. Can we bring up Government's Exhibit 1440? And what is Government's Exhibit 1440?

A. This is a log of questions that potential money mules had asked and information about them.

13:49:40 **Q.** And where did you find this?

A. On the command and control server.

Q. Okay. Okay. Let's's take it down. I want to talk about a different topic now, which is how you saw the Bayrob Group communicate. Now, first -- and it's just a yes or no question -- did you see the Bayrob Group communicate amongst each other? 13:50:10

A. Yes.

Q. All right.

And I'm going to break this into three different categories, and I'm going to ask you about them separately. 13:50:18

So I want to talk to you about Bayrob members communicating with the botnet through the command and control server. That's one category. Same category is Bayrob members communicating with victims. And the third category is 13:50:37 Bayrob members communicating with each other. Okay. So first I want to start with that first category, Bayrob members communicating with the botnet, the infected computers through the command and control server. Okay.

First I want to make sure we're all talking about the 13:50:54 same thing. What's a botnet?

A. Botnet is a collection of infected computers.

Q. And who controls that collection?

A. The owner of the botnet, the person who's infected those computers.

13:51:10 **Q.** Okay. And you say owner, but is it the owner of those computers?

A. No, it's the creator of the virus.

Q. Okay.

And is there any limit to how many infected computers 13:51:23 can be in one botnet?

A. No.

Q. Roughly how many infected computers did you see in the Bayrob botnet?

A. 400,000.

13:51:33 **Q.** And was that over time?

A. Yes.

Q. So, in other words, at any given moment, there might not be 400,000?

A. Correct.

13:51:43 I'd like to show you a Rule 2006 summary, Government's Exhibit 1873.

MR. O'SHEA: You say 1870 -- okay. Okay.

BY MR. LEVINE:

Q. What is Government's Exhibit 1873?

13:52:08 **A.** This is a diagram of how the infected computers were controlled.

Q. Okay.

And does this exhibit fairly and accurately summarize the structure of the Bayrob botnet as it existed during the certain time period? 13:52:24

A. Yes, it does.

Q. And would the data from which this diagram was created, the various servers and the communications between those servers, would that be too voluminous and complex for the jury to reasonably review at trial? 13:52:36

A. Yes, it would.

Q. Would this diagram help explain how the Bayrob Group botnet was structured?

A. Yes.

13:52:46 **Q.** Okay.

So looking at the top of Government's Exhibit 1873, the top refers to command and control server or C and C servers there. Will you please remind us what a C and C server is?

13:53:00 **A.** That's the computer where the infected machines will be sent instructions that could be commanded and controlled from that computer.

Q. And what is a server exactly?

A. It's a computer that is available online 24/7, a
13:53:20 powerful computer.

Q. And where did you see the Bayrob command and control servers being hosted?

A. I saw them being hosted at Dream Host.

Q. What is Dream Host?

13:53:32 **A.** Dream Host is a company that will host -- a company that will give you a computer to use the Internet.

Q. And that computer is called a server?

A. Yes.

Q. And where physically are Dream Host servers located?

13:53:45 **A.** I believe in a lot of places, but certainly they have one in Los Angeles.

Q. Okay.

But they may have data centers in other locations as well?

13:53:55 **A.** Yes.

Q. Now, can you explain what was in between the top level command and control servers there and the infected computer, what's the next row down we see?

A. The next row down is relay servers.

13:54:07 **Q.** What are relay servers?

A. So relay servers are servers that will pass information from the command and control server through them and out to the infected computers.

Q. And where did you see the Bayrob relay servers being hosted? 13:54:28

A. Hosted in many different locations but Yahoo was one of the hosts.

Q. Okay.

And why have relay servers? What's the purpose of having a multi-layer structure like this? 13:54:38

A. For security companies such as Symantec we try to approach Yahoo and ask them to remove a server if it's doing something malicious. And so if we see activity coming from a computer, malicious activity coming from a computer that's hosted at Yahoo, we can go to Yahoo and ask them to take 13:55:01 that machine offline or to investigate it, and malware authors know this.

So they know that their computer they're using to control their no -- the infected machines will be taken away from them. So what they do is they have multiple of these, 13:55:20

what we're calling relay servers. And so that if one gets taken down, another one can be used instead immediately.

And also if that was their main command and control center, it would be difficult for them to restore connection 13:55:42 to all of the infected machines.

So they have this system of relay servers to protect them against investigators and others such as myself.

Q. But -- so having the relay servers among other things, does it make it more difficult to locate the command and 13:56:07 control servers?

MR. O'SHEA: Objection.

THE COURT: Overruled.

THE WITNESS: Yes, it does.

Q. But you were able to locate the Bayrob Group's top 13:56:16 level command and control server?

A. Yes, I was.

Q. All right.

Now you mentioned at some point that they used domain names, Bayrob Group used domain names so that the infected 13:56:29 computer could speak with a command and control server.

Can you explain how that works?

A. They have the name of the website that is going to be controlling the virus. They have that embedded in the virus. So when the virus runs on the victim's computer, it 13:56:48 will look inside itself to find the domain name, where it should connect to receive instructions.

Q. Okay.

So -- and then it reaches out and receives the instructions?

13:56:59 **A.** Yes.

MR. O'SHEA: Objection.

THE COURT: Sustained to the form of the question.

BY MR. LEVINE:

13:57:06 **Q.** What happens once it gets -- once it figures out a domain name?

A. The virus knows that it needs to connect out to that domain name and see if there's any instructions awaiting for us so they can take action on the victim machine.

13:57:21 **Q.** Now, hard coded into the virus, was there at least initially a static list of different domains?

A. Yes.

Q. What do we mean by a static list of domains?

A. A list that doesn't change so there's -- there's hard 13:57:42 coded domain names in the virus, and what the virus does is it goes to that list, generate about five domain names in there, and will go through that list as we'll try to connect to the first one. And if that fails, it will try to connect to the second one, and so on, until -- repeatedly until it 13:58:02 finally receives instructions about what to do.

Q. What is -- is there a problem from a criminal's perspective with having a static list of domain names like that listed in the malware?

A. Yes, it is.

13:58:14 **Q.** What is the problem with that?

MR. GOLDBERG: Objection.

THE COURT: Was there an objection?

MR. GOLDBERG: Objection, your Honor.

THE COURT: I'm sorry?

13:58:21 MR. GOLDBERG: Objection.

THE COURT: Overruled.

THE WITNESS: Yes, there is a problem.

Q. What is the problem?

A. This is a known problem for malware authors, and the 13:58:32 problem is that researchers, security companies, and identifier companies will analyze the virus and they will get that list of domain names out of the virus, and then we will contact all of those websites, the hosters, who are hosting those websites, and we will ask those companies to 13:58:54 take those websites offline. And if all of those websites go offline at the same time, then the virus can no longer connect to -- no longer receive instructions.

So the virus authors, they lose control of all of their infected machines and they can't get that back, so.

13:59:14 **Q.** So did the Bayrob Group do something to prevent this over time?

A. Yes, they did.

Q. What was the first thing they did to prevent their command structure being taken down?

13:59:28 **A.** So the first thing they did was they -- they added more domain names in there and they started to create domain names, not from a static list but they would create them on the fly from word lists instead.

Q. So explain how that would work.

13:59:48 **A.** So for static name, you know, the name could be badguy.com, and I can read that in the code and I can know what it is. So instead of having that hard coded into the virus, what they did was they had two groups of words, and they would choose a word from the first list, and then they 14:00:11 would choose a word from the second list, and it would put those together. And then that would be the domain name they would use to connect out to receive instructions. And the benefit of doing that is that you can have a very long list of words. And so you can create thousands or tens of 14:00:32 thousands of domain names for the virus to connect to. And that makes it very difficult for security researchers or antivirus people to go and connect to find out where all 10,000 of those domains are and to ask the companies to take down all 10,000, just becomes too big of a problem.

14:00:54 **Q.** So -- but wouldn't they have to buy 10,000 different domains, register 10,000 different domains?

A. No. So they don't have to do that. All they have to do is know what the main -- what words are going to be chosen from that list, and then they will pick one of those 14:01:11 combinations and they can register that one combination and then just have to wait over time for the virus to eventually get to that combination. And when the virus gets to that combination, it will then start receiving instructions from that domain.

14:01:25 **Q.** Okay.

So this is something that's done to make it harder to disrupt a botnet?

MR. GOLDBERG: Objection.

THE COURT: Sustained.

14:01:38 **Q.** Why is this method used?

A. It's done to protect the botnet so that the creator of the virus author doesn't lose control of all the infected machines.

Q. Okay.

14:01:50 So you said this was one step that the Bayrob took to make it harder to describe the botnet. Was there another step as well?

A. Yes, there was another step.

Q. What was the other step?

14:02:02 **A.** The other step was they came up with a different way to communicate with the infected machines. This method is well known to virus authors, and more secure way to communicate with infected machines. And it's called peer-to-peer communication. And the way it works is that 14:02:25 instead of the infected computer needing to reach out to one command and control server, instead of that, they have a mechanism where an infected computer can reach out to another infected computer, and they can ask that computer, "Do you have any instructions that I -- that I should have?" 14:02:45 And the infected computers themselves will exchange the instructions between each other. And this means that it's no central location as far as security researchers to target and to take down and it makes the botnet resilient to researchers being able to disrupt it.

14:03:07 **Q.** Okay.

I'm going to show you what has been previously marked as Government's Exhibit 1441.

MR. O'SHEA: Objection. May we approach on this one, Judge? I apologize.

14:03:28 (The following proceedings were held at side bar:)

THE COURT: You took it down? Okay. Thank you. Would you please put it back up for me. Oh, all right.

(The following proceedings were held at side bar:)

14:04:01 MR. O'SHEA: What I anticipate, Judge, based upon what I remember from our conversation last night is this is a list of domain names that were essentially acquired illegally or by theft or what not. This tracks the enhancement in the indictment.

14:04:23 THE COURT: Um-hum.

MR. O'SHEA: Okay. Almost word for word, chart for chart. So this is a self-created document. I don't -- you know, he can talk about certain domain names by name and I don't want to be picky here, but I'm not
14:04:36 conceding this issue. It's a big one in the case. It's not a minute one. It's the entire enhancement. They're going to try to get in through, you know, multiple errors of what I think is hearsay, so.

THE COURT: Was this document prepared by him?

14:04:51 MR. LEVINE: No.

THE COURT: Tell me.

MR. LEVINE: So this is just Paragraph 1 of the table, Paragraph 168 of the indictment.

And the question I'm going to ask him is --

14:05:00 THE COURT: Well I should -- I apologize. I shouldn't have said prepared by him. Prepared by the Government.

MR. LEVINE: It was prepared by the Government.

14:05:10 THE COURT: Yeah.

MR. LEVINE: So --

THE COURT: But he's a witness --

MR. LEVINE: Paragraph 168, it's the table from Paragraph 168 in the indictment. The question I'm 14:05:19 going to ask him is -- the question I'm going to ask him is did he see his infected computer reach out to all of those domains, and he's had this in advance and he's looked at it and will confirm he saw his infected computer reach out to all of those domains. And that's the only question I'm 14:05:37 going to ask him.

THE COURT: Oh.

MR. O'SHEA: Foundation.

MR. LEVINE: I'll lay a foundation.

THE COURT: What's the problem with that?

14:05:46 MR. O'SHEA: I just -- I don't think -- well, obviously, Judge, the jurors aren't going to memorize this chart. Got it. But I don't want this question to get -- to be presumed that we are agreeing to the admission of this exhibit at all at the conclusion of this case, period. In 14:06:07 order to refresh his recollection and everything else, oh, yeah, fine, publish it, but not -- not an exhibit for admission, in my opinion.

THE COURT: Okay.

So you're not objecting to the jurors seeing this 14:06:20 list; you are objecting to its admissibility?

MR. O'SHEA: Absolutely. Not objecting to -- the witness using it to refresh his recollection about how many and what not. Okay.

THE COURT: I am going to permit you to refer 14:06:39 to Paragraph 168. I'm going to allow you -- him to look at this. I'm going to allow the jurors to see it as well. I will not opine on admissibility at this point in time.

MR. O'SHEA: Okay. Fair enough. Thank you, Judge.

14:06:57 THE COURT: It -- in other words, I'm not going to opine on whether it's appropriate to just simply take out a portion of the indictment and highlight it as -- as an exhibit. I just want to remind everybody we were all in agreement that the jurors were going to get a copy of the 14:07:19 indictment. So I want that for the record because we all agreed in advance of the trial that they at the end would get a copy of the indictment.

MR. O'SHEA: Fair enough.

MR. LEVINE: You're right, your Honor. The 14:07:31 only alternative way -- the only alternative way would be to ask about each domain name individually. So it's just to save time.

THE COURT: And I like that.

MR. O'SHEA: I do too normally, but I can't at 14:07:44 this time because --

THE COURT: You're allowed.

MR. O'SHEA: Okay. All right.

THE COURT: Thank you.

(Proceedings resumed within the hearing of the jury:)

14:08:20 THE WITNESS: I don't see anything on my screen.

THE COURT: One moment, sir.

THE WITNESS: Okay. Thank you.

BY MR. LEVINE:

14:08:27 **Q.** Mr. Omurchu, is it up on your screen?

A. Yes, it is now. Thank you.

Q. Okay.

So Exhibit 1441 is a two-page exhibit. I'm going to hand you a copy of both pages, and I will represent to you 14:08:48 that this is a list of domain names that I extracted from Paragraph 168 of the indictment. If you could show the next page, too, as well to the jury.

Mr. Omurchu, did you have an opportunity to review this list before taking the stand today?

14:09:12 **A.** Yes, I did.

Q. Okay.

And looking at this list from Paragraph 168 of the indictment, did you see the infected computers that Symantec had communicating through each of these domain names?

14:09:29 **A.** Yes, I did.

Q. Okay. Let's take it down. So now I want to talk -- we were going to talk about three types of communications. I want to talk about the second type of communication now, which is communications between the Bayrob Group and 14:09:51 victims. So I want to talk about how the Bayrob Group would communicate with victims, such as eBay fraud victims or money mules.

Would the Bayrob Group just e-mail eBay fraud victims or money mules directly from their home IP address?

14:10:05 **A.** No.

Q. How would the Bayrob Group e-mail eBay fraud victims or money mules?

A. They would use accounts that they had created and they would send the traffic through -- they would connect through 14:10:23 the infected machines at the proxies before they would send e-mail.

Q. Okay.

And was your computer one of the infected computers that they would proxy through?

14:10:33 **A.** Yes, it was.

Q. And can you just remind us what it means to proxy through a computer?

A. It means that someone can connect in to my computer, and they can forward the request out on the other side of my 14:10:47 computer. And when the request comes out, it -- it has the address of my computer. So the origin of the request is masked.

Q. Okay. Let's bring up Government's Exhibit 1443. And if we could zoom in. All right. And if we need to zoom in to a particular portion, let me know, Mr. Omurchu. 14:11:27

What is Government's Exhibit 1443?

A. This is a log of the traffic that was coming through my infected machine.

Q. I'm sorry. This is -- could we go to Page 1? Okay.

14:11:59 This is Page 1 of Government's Exhibit 1443. And what are we seeing here on Page 1?

A. So on Page 1 this is a -- the program you see in the background is Wire Shark, the program that I used to record the traffic that is going through my machine.

14:12:14 And in this case, the traffic that you've recorded is asking my machine what other machines can I connect -- can the attackers connect to from my machine.

Q. Okay.

So this is showing us Exhibit 14 -- is Exhibit 1443 showing us what the attacker is doing on your computer? 14:12:37

A. Yes.

Q. And is this something that I would be able to see if I just -- if it was happening on my infected computer?

A. No.

14:12:49 **Q.** Why are you able to see it?

A. Because I'm monitoring with the security tools.

Q. Okay.

And what is that where it says "list slots" in red?

A. So this slot is a command you can send to my infected 14:13:03 computer. And in this case, it has been sent to my computer.

Q. What does it do?

A. So when my infected computer receives that command, and it will ask for a password, and the -- that's my machine 14:13:20 responding with the password in blue text. And then the remote machine is sending the Password 213D1400, and when the password is confirmed by my infected machine, what is sent back is a list of other machines that you can connect to via my machine.

14:13:43 So these are other infected machines, and they are available to be used as proxies.

Q. So this is actually proxying that we're seeing?

A. Yes.

Q. Over your infected machine?

14:13:56 **A.** Yes.

Q. And who's proxying here?

A. The Bayrob Group.

Q. And what are the IP addresses that we see at the bottom of the screen there?

14:14:07 **A.** Those are other infected machines.

Q. So they're the IP addresses of other infected machines?

A. Yes, those are the addresses of the other infected machines.

14:14:17 **Q.** And what is that string of letters and numbers to the left of the IP addresses?

A. That's the password for the machines.

Q. Okay.

Now, is this program organically on your computer or 14:14:47 was this part of the malware?

A. This is part of the malware.

Q. Okay.

Could you zoom out to the full thing here? Could we go to Page 2 now, and if you'll zoom in. Thank you. Okay. 14:15:15 So what are we seeing in this view, on Page 2?

A. So in this view, we're seeing the command -- my infected machine. The virus on my machine is receiving the command "select socks.

Q. And what does the command "select socks mean?

14:15:32 **A.** Well the word socks is a word used to describe a proxy, it's -- a technology that allows you to communicate with the proxies. And so in this case, they're saying they want to select another machine to connect to from my machine.

14:15:56 **Q.** And how is socks in this context for proxying, how is that typically spelled?

A. It's typically spelled S-O-C-K-S, like socks on your feet.

Q. Like socks on your feet?

14:16:11 **A.** Socks on your feet, yes.

Q. Okay.

And where did the command select socks come from in the screenshot?

A. It came from the Bayrob server.

14:16:30 **Q.** Okay. So it came from whoever was proxying into your machine?

A. Yes.

Q. Did the Bayrob Group also have a way of directing infecting computers, infected computers to form a proxy 14:16:46 network with network?

A. Yes.

Q. What does a proxy network mean in this context?

A. A proxy network is a chain of proxies. So to protect your location, if you just went through one proxy, then 14:17:09 there's a possibility that whoever is listening on that proxy knows where you're coming from because they -- if you're sitting on the computer, you will see the original address of the person connecting to your machine.

So the benefit of a proxy networker, a chain, is that 14:17:25 you connect through multiple infected machines. So you might go through three infected machines, which means that if I want to understand where the true origin of that request is coming from, I would have to be sitting on all three of those machines, and I would have to see where 14:17:42 the -- exactly how the chain works.

So going through multiple proxies makes it very difficult to understand where the person behind that is sitting, and it's a technique that's used very commonly for people to stay anonymous online so they can't be traced.

14:18:00 Particularly, if you use proxies that are in multiple countries, and if you wanted to track the traffic across those countries, you'd have to be present in all of those countries or have cooperation from those countries in order to be able to trace exactly where the origin is coming from, 14:18:18 sort of like what you see in the movies where they're trying to trace the connection back.

Q. Okay.

So were you ever able to do that, were you ever able to get on all the different proxies in the chain and trace 14:18:31 it back?

A. Yes, I was.

Q. Explain.

A. Because I had multiple infected machines, there were -- there was occasions when the Bayrob Group happened 14:18:49 to select all of my machines in a chain, and then I could see the chain from beginning to end. I could see the connection from beginning to end.

Q. And where did you see it end?

A. In Romania.

14:19:02 **Q.** Were you able to determine any more detail than in Romania?

A. Yes, I saw connections coming from Bucharest and from town called Brasov in Romanian.

Q. Any other detail than those two towns or Bucharest, I 14:19:21 would say more of a city, towns or cities?

A. I mean I -- I'm -- no.

Q. That's okay. All right. So I want to show you what's been previously marked as Government's Exhibit 1442. And if we could zoom in on the map portion of this.

14:19:59 What is Government's Exhibit 1442?

A. This is a map I made of the locations of the computers that I was asked -- my infected machine was asked to connect to.

Q. Okay.

14:20:14 How did you know the location on the computers that your machine was asked to connect to?

A. Because I was sent to a list, my infected machine was sent a list of other computers, and that -- that were infected, and that could be changed together, and I was able 14:20:34 to collect that list of the addresses of those infected machines, and then using that -- the address of those machines, I was able to map them out to show where they are on the map here.

Q. When you say addresses, are you talking physical address or IP address? 14:20:48

A. Talking IP address.

Q. So how can you go from an IP address to a real world location?

A. So IP addresses are assigned out to different companies. 14:21:00 And there's a central repository that keeps the IP address and the company associated together, and the companies also provide location information. And so there's essentially a worldwide database that shows you where IP addresses are located in the world.

Q. Okay. 14:21:23

And does it -- how granular does the location information get? Is it a street address, is it a town, is it a country?

A. It depends, but it can get as accurate as the exact building that you're sitting in. 14:21:37 And sometimes, it will give you the town, and sometimes it will give you the country, and there's different levels of granularity but it can be the exact spot you're in.

Q. Okay.

14:21:50 And what level of granularity did you find in the IP addresses of the infected machines when you looked up their locations?

A. Well, what I found that was interesting was that the IP addresses were located in mostly two different countries, 14:22:08 in the United States or in Romania.

Q. And why was that interesting to you?

A. It was interesting because I knew there was Romanian words in the virus. So I felt that the virus had some Romanian connection already and then to see the infected 14:22:24 computers were -- that I was being asked to connect to were only in the United States and Romania made me think that the operators of the Bayrob virus were in Romania.

Q. Okay.

And did you -- did you plot these red points on this 14:22:42 manually or did you use some kind of program to do that?

A. No, I used a program to do it.

Q. And has the software that you used to plot that IP information been accurate and reliable in the past?

A. Yes, it has.

14:22:54 **Q.** And Symantec regularly relies on this type of software to plot graphic locations of IP addresses?

A. Yes.

Q. All right. Let's bring this down.

So now I want to talk about the third kind of 14:23:15 communications, the last type of communications that I wanted to talk about. And that's communications between the Bayrob Group.

First of all, do you know some of the ways the Bayrob Group would communicate with each other?

14:23:27 **A.** Yes, I do.

Q. Okay.

How do you have an understanding of how the Bayrob Group would communicate with each other?

A. Because they were sending the traffic through my infected machine. 14:23:36 So I could watch the traffic that was coming through my infected machine, and by looking at what was happening there, I could see that some of that traffic was communication between members of the group.

Q. Okay.

14:23:48 Was one of the ways that you saw the Bayrob Group communicating through your infected machines e-mail?

A. Yes.

Q. All right.

I want to bring up Government's Exhibit 1444. What is 14:24:10 Government's Exhibit 1444?

A. It's an e-mail that I saw that -- it's a screenshot of traffic that was coming across my infected machine, and it shows an e-mail.

Q. Okay. And who is the sender of this e-mail?

14:24:26 **A.** The sender of the e-mail is MasterFraud.

Q. MasterFraud at what e-mail account?

A. MasterFraud@GMX.com.

Q. What is GMX.com?

A. GMX is a German mail provider.

14:24:40 **Q.** Similar to gmail or Yahoo mail or anything like that?

A. Yes.

Q. And who are the recipients of this e-mail?

A. The recipients of this e-mail are Amightysa@zoho.com, linxstyle@GMX.com, Minolta9797@GMX.com, natiune@GMX.com, and natiune@GMX.com. 14:25:05

Q. Okay.

One of those is at zoho.com, Amightysa@zoho.com. Do you know what zoho.com is?

A. No, I don't.

14:25:14 **Q.** Okay. But, based on a format of that -- of that information, does there appear to be an e-mail provider?

A. Yes.

Q. What is the subject line of this e-mail?

A. The subject line is money mole.

14:25:29 **Q.** Okay.

And were you able to obtain the content of this e-mail?

A. No, I was not. I was able to obtain encrypted content, not the readable -- not the readable content.

14:25:51 **Q.** All right.

Let me ask you have you seen other e-mails through your infected machine between those same e-mail addresses?

A. Yes, I have.

Q. Roughly how many e-mails between MasterFraud, AmightySA, and Minolta 9797 would you say you've seen? 14:26:06

A. Many. I don't know. I couldn't put a number.

Q. Are we talking --

MR. GOLDBERG: Objection, objection.

Q. -- tens, hundreds, thousands?

14:26:23 THE COURT: Overruled. Would you answer that last question, sir?

THE WITNESS: Hundreds.

BY MR. LEVINE:

Q. Okay.

14:26:32 And were these monikers basically the same in all of those hundreds of e-mails?

A. Yes.

Q. But did the Bayrob Group members sometimes change providers in terms of which e-mail provider they were using?

14:26:46 MR. GOLDBERG: Objection, form.

THE COURT: Sustained.

Q. Were the -- did the Bayrob Group always use GMX and zoho.com to use these monikers?

MR. GOLDBERG: Objection.

14:27:00 THE COURT: Sustained.

Q. What e-mail providers did you see these monikers coming from?

MR. GOLDBERG: Objection.

THE COURT: I'm sorry. Was there an objection? 14:27:11

MR. GOLDBERG: Objection.

THE COURT: Overruled. You may answer that.

THE WITNESS: I saw them coming from multiple different providers. I believe yahoo.com was another.

14:27:24 **Q.** Okay.

And were the content of all of the e-mails you just described encrypted?

A. Yes.

Q. And what does it mean when an e-mail's content is encrypted? 14:27:39

A. It means that it's protected, and you can't read it unless you know the password to decrypt it.

Q. Did you know the password?

A. I did not know the password.

14:27:53 **Q.** Are there different types of encryption?

A. Yes, there are.

Q. What kind of encryption was the Bayrob Group using in these e-mails?

A. They were using an encryption, which is known as PTP, stands for pretty good privacy. 14:28:07

Q. Pretty good privacy?

A. Yes.

Q. Did Symantec have the ability to crack that kind of encryption?

14:28:16 **A.** No, we do not.

Q. But it's only pretty good privacy?

A. That's the name that the program was given.

Q. But you still don't have the ability to crack it?

A. No.

14:28:27 **Q.** Were the subject lines and attachment names of those e-mails encrypted?

A. No, they were not.

Q. Were some of the subject lines and attachment names you saw in Romanian?

14:28:37 **A.** Yes, they were.

Q. All right.

And having seen hundreds of e-mails, such as Government's Exhibit 1444, do you have an understanding -- a general understanding as to MasterFraud, AmightySA and Minolta9797's role in the Bayrob Group?

14:28:55

MR. GOLDBERG: Objection.

THE COURT: Overruled.

THE WITNESS: Yes.

Q. What understanding do you have as their role in the group?

14:29:04

MR. GOLDBERG: Objection.

THE COURT: No, overruled. Go ahead, sir.

THE WITNESS: It appeared that MasterFraud was the name sender, and that Minolta and AmightySA were receiving e-mails mostly. 14:29:19

Q. Did you have a sense of whether these were high level members of the group based on the e-mails you reviewed?

MR. GOLDBERG: Objection.

THE COURT: Sustained.

14:29:32 **Q.** Okay.

So one of the ways the Bayrob Group would communicate was through encrypted e-mails. Was another way the Bayrob Group communicated with each other for a time through Yahoo, through Yahoo draft messages?

14:29:48 **A.** Yes.

Q. Okay.

And yes, can you take this down. Thank you. Oh, can you keep it up for a second?

Oh, there's an X-mailer header there at the top. What's an X-mailer header? 14:30:06

A. It tells you about the mail program that was used to send the e-mail.

Q. That tells you what e-mail program they're using to send the e-mail?

14:30:20 **A.** Yes.

Q. And what mail program were they using to send the e-mail?

A. RoseCitySoftware.Com. Courier is the name at the beginning, and version number, and then after that is 14:30:31 RoseCitySoftware.Com.

Q. And courier is -- there's a version number after it?

A. Yes.

Q. Is that 3.50.00.09.198?

A. Yes, it is.

14:30:44 **Q.** Besides seeing the Bayrob Group use this mail program, have you -- had you ever seen it before?

A. No, I had not.

Q. So we're talking about Yahoo draft e-mails. How would the Bayrob Group communicate through Yahoo draft e-mails?

14:31:13 **A.** So the draft -- can I rephrase that? I don't think it was quite draft the e-mail.

Q. So how did they communicate using Yahoo besides e-mail?

A. So there was a feature in Yahoo called Notepad.

14:31:34 **Q.** Okay.

A. So when you went into your Yahoo e-mail, you could click on the Notepad option, and that gave you a little Notepad that you could write notes in. And what I observed was that multiple different personas would log into the same 14:31:54 Yahoo account, and they would leave messages for each other in that Notepad part of the Yahoo account.

Q. So no communication was ever sent?

A. Yes.

Q. Different people would just log onto the same account and view the same Notepad? 14:32:09

A. Yes.

Q. All right. If we could bring up what's been previously marked as 1445.

What is Government's Exhibit 1445?

14:32:27 **A.** And this is information that that was in the Yahoo Notepad of one of the accounts, and I saw this because they -- a member of the group accessed this Notepad while they were proxying the traffic through my machine.

Q. Okay.

14:32:50 And do you have, based on your investigation, do you have an understanding of what this information on this Notepad is about?

A. Yes, I do.

Q. What do you understand it to be about, based on your investigation? 14:33:05

A. It's been money mules.

Q. Can you elaborate?

A. Well, in particular, if you look down three quarters of the way down, you see three new 10 June picked. Crystal Hart from Goodyear Arizona, is the money mule that I was 14:33:21

asked to use when I did my operation to buy a car. So I
know that Cristol Hart is a mule. And if you see the
number -- the dollar amount at $2900, three times, that --
and comes out roughly to the price of the car that I was --
14:33:47 that I bought. And then also the -- there are numbers here
as well that correspond to Western Union transaction
numbers, and I was able to put those transaction numbers
into Western Union and able to see the transactions that had
occurred.

14:34:07 And the name -- in this particular case, Cristol Hart,
and let's say the last name there, Peros Scabor was the name
of the recipient who Cristol Hart had sent $2900 to, via
Western Union.

Q. So Cristol Hart, when we looked at that eBay video,
14:34:30 your undercover operation?

A. Uh-huh.

Q. Where was -- Cristol Hart was in that video?

A. Yes.

Q. Where was she in that video?

14:34:38 **A.** At the end when I was given an agent, an eBay agent to
transfer my money to, the eBay agent was Cristol Hart in
Goodyear, Arizona.

Q. Could we go back to Exhibit 1435 and just to the end
of the video? So can you show us where it's referring to
14:35:44 Cristol Hart?

A. Here, here Cristol Y. Hart, and her address is 13470 West Van Buren Street in Goodyear, Arizona.

Q. If we could go back to the Yahoo Notepad, 1445.

Okay. So where it says there, "Three new 10JUN 14:36:20 picked," did you have an understanding of what that means based on your investigation?

A. Yes.

Three new transactions from a money mule on the 10th of June.

14:36:33 **Q.** Okay.

And each amount is exactly the same. Do you have understanding of why that is?

A. The money mules were given instructions to receive the full amount from the auction and to split it into three 14:36:48 equal transactions and then to send that money via three different Western Union officers and three different transactions, three different people.

Q. Okay.

And could we go back to the whole -- same exhibit.

14:37:13 Now at some point on this Notepad, does the Bayrob Group actually refer to mules towards the top?

A. Yes.

Q. Okay.

Now, did -- this is what was in the Notepad. You 14:37:35 didn't add this?

A. No.

Q. Okay.

So let's bring this down. You've seen the Bayrob Group communicate with each other via encrypted e-mail and Yahoo Notepad. 14:37:56

Did the Bayrob Group also communicate with each other over a chat application?

A. Yes, they did.

Q. What chat application did you see the Bayrob Group using? 14:38:07

A. I saw them use Jabber. Pigeon is the name of the program, Jabber, and -- yep.

Q. So what is -- let's go through this. What is Pigeon?

A. It's a chat program.

14:38:23 **Q.** Can you elaborate on that?

A. It's like a program you would have on your computer to chat with other people, like Yahoo Messenger is a very common one, or MSN, MSN Messenger, any messenger program that allows you to talk with somebody else.

14:38:43 **Q.** Okay. And what about Jabber? What is Jabber?

A. Jabber is a way that -- a way to communicate, just different ways to communicate Jabber is the way you can communicate.

Q. So would it be possible to use a Pigeon application to do Jabber chat? 14:39:01

A. Yes.

Q. What would that mean?

A. It means that you have a program on your computer you can go to and type your message into, and as long as the 14:39:16 recipient has the same program and is in your contacts, you can communicate with them. And the way you're communicating is if you have Jabber.

Q. And the program is called Pigeon?

A. Yes.

14:39:27 **Q.** By -- you said you could do that with the computer. Could you do that also with a cellphone?

A. I believe so.

Q. Okay.

And if one wanted to conceal his communications from 14:39:40 law enforcement, are there any benefits to using Jabber?

A. Yes, the main benefit is that you can install an encryption add-on on top that will encrypt all your chats so that they can't be read if they're intercepted.

Q. Okay.

14:39:58 And what about does Jabber give you the ability to use a private Jabber server?

A. Yes, it does.

Q. What is a private Jabber server?

A. So in chat programs, when you send a message, the 14:40:13 message often goes to the company who is running that chat program. So, for example, with Yahoo, the chat can go from your computer to the Yahoo computers servers, and then back out to the person who you're trying to talk with.

And what a private Jabber service allows you to do is 14:40:38 allows you to not have to go through a central company like Yahoo, and instead, you can go to the private server you set up. And that's good because it means that there's less chance to intercept the communication.

So, for example, Yahoo could intercept the 14:40:54 communication with you're having a Yahoo Messenger conversation. But using a private Jabber service, there's less chance of interception to happen.

Q. Where would the private -- where could a private Jabber service be located?

14:41:08 **A.** You can run it anywhere on your home computer if you want. Any computer that's connected to the Internet.

Q. Okay.

You have any visibility as to whether or not the Bayrob Group was using their Pigeon application to do Jabber 14:41:23 chat or some other format of chat?

A. Yes.

Q. What -- what form of chat were they doing?

A. They were doing off the record type of chats.

Q. Okay.

14:41:35 So you said something new there. But, first were they doing Jabber chat or Pigeon?

A. Yes.

Q. And were the Bayrob Group chance over Pigeon encrypted?

14:41:47 **A.** Yes.

Q. What type of description was the Bayrob Group using for chats over Pigeon?

A. A program called Off the Record.

Q. Off the Record?

14:41:58 **A.** Yes.

Q. Is that abbreviated in some way?

A. It is. It's abbreviated to OTR.

Q. OTR as in record?

A. Off the Record, yes.

14:42:07 **Q.** All right.

What is Off the Record encryption?

A. It's a way to send your messages so that they're protected and they can't be read, except by the parties who are sending and receiving the message.

14:42:26 **Q.** And does OTR encryption come with Pigeon or is it something you have to add on yourself?

A. You add it on yourself.

Q. Does Symantec have the ability to crack OTR encryption?

14:42:38 **A.** No, we do not.

Q. Attachments sent through Pigeon, are those encrypted?

A. What I saw was that the attachments were not encrypted.

Q. Okay. I'd like to show you what's been --

14:42:53 THE COURT: You know, we're going to take a break at this point.

Folks, remember the admonition. All rise -- and ladies and gentlemen, we will be recessing at 4:30 today or adjourning at 4:30 today.

14:43:05 All rise for the jury.

(Thereupon, a recess was taken.)

THE COURT: You may continue.

MR. LEVINE: Thank you, your Honor.

BY MR. LEVINE:

15:10:36 **Q.** So just a quick recap where we were before, you were -- did you testify that you saw encrypted chat between members of the Bayrob Group over your infection?

A. Yes, I did. And I need to make one correction there, though.

15:10:53 **Q.** Okay. Go ahead.

A. The encrypted chat that I saw, that I personally saw, was not over Jabber; it was over AOL Instant Messenger.

Q. AOL Instant Messenger?

A. Yes, with the OTR program on top, the encryption program on top. 15:11:09

Q. Okay.

And was the program Pigeon involved at all?

A. Yes.

Q. How was the program Pigeon involved?

15:11:16 **A.** Pigeon was the client -- the program on the computer that was being used to send the messages.

Q. So a member of the Bayrob Group used a Pigeon program on their computer to have chats over AOL Instant Messenger?

MR. GOLDBERG: Objection.

15:11:34 MR. O'SHEA: Objection.

THE COURT: Sustained.

Q. Can you explain how this would -- how this chat would happen on the perspective of the user?

A. Sure. You would have a Pigeon program running on your 15:11:46 computer, with the Off the Record plug-in on top to encrypt the messages. Then you would log into your AOL Messenger and you would send messages but when your messages are sent, they were encrypted.

Q. All right.

15:12:03 And you saw those encrypted messages over your --

A. Yes.

Q. Sorry. Let me finish the question. Encrypted messages over your infected computer?

A. Yes, I did.

15:12:13 **Q.** Okay.

I want to show you what's been marked as Government's Exhibit 1446. All right.

I'm -- so what is Government's Exhibit 1446?

A. This is an image that was transferred between Bayrob members while they're using my computer as a proxy. 15:12:48

Q. Okay.

And was this image encrypted?

A. This message was not encrypted.

Q. Is that why we're able to see it today?

15:13:02 **A.** Yes.

Q. All right.

And who sent -- what moniker sent this message to what moniker?

A. This message was sent from the moniker, QWWXX, to the moniker, Minolta 9797. 15:13:15

Q. Okay.

And there are two pages to this exhibit. Can we just take a quick look at the second page so the witness can see? Okay. Let's go back to the first page. We'll get to the second page later. 15:13:33

Was the second -- was that second page also sent through -- just strike that.

Were the screen shots sent on or about April 4, 2013?

A. Yes.

15:13:49 **Q.** Okay. And you got them through your infected computer?

A. Yes.

Q. All right.

So let's start by looking at this first page. What does this screenshot appear to show? 15:14:04

A. This shows someone's computer. They -- what's called a desk top on their computer.

Q. All right. What is a desk top?

A. It's the main thing you see when you turn on your computer. 15:14:21

Q. Okay. All right.

So does this screenshot of the desktop give you insight into how the Bayrob Group operated?

A. Yes, it does.

15:14:38 **Q.** All right.

So first, looking at the bottom right, what date and time does this screenshot appear to have been taken?

A. April 4, 2013 at 8:10 P.M.

Q. Now next to the date and time, there's a gold and brown box with a T in it. 15:14:55 Can you zoom -- can you zoom into --

THE COURT: Did you say with a T in it?

MR. LEVINE: It's very hard to see there. Yes.

15:15:14 **Q.** Do you know what that represents, that if you could point to it with the arrow. Okay. Do you know what that represents?

A. Yes, that is the icon for, it's a little blurry but it appears -- I recognize as the icon for Trucrypt.

15:15:30 **Q.** What is Trucrypt?

A. Trucrypt is a program that allows you to encrypt your entire hard drive.

Q. Can you also use it to encrypt a portion of your hard drive?

15:15:41 **A.** Yes, you can.

Q. All right.

And to the left of that gray box, two to the left or to that gold box, the one all the way to the left there, where you're pointing right there. Thank you.

15:15:53 It's a little gray box appears to say VM. Do you know what that represents?

A. Yes, that represents a virtual machine software.

Q. All right. What is a virtual machine?

A. Virtual machine is a machine that you can run inside 15:16:14 of another machine. So normally when you turn on your computer, you're running it on the hardware that's actually, you know, the hardware is actually on your desk. What you can do then is have a second computer -- a second computer running inside of that, and it's isolated from your real 15:16:40 computer. And you can install different software in there.

You could do completely different work inside of the virtual machine and it would have no effect on anything outside of the virtual machine. It's a way to isolate your work so that work you do one place doesn't bleed out into your real machine. 15:16:59

Q. Okay.

So you can keep -- so you can keep one work flow or stream within the virtual machine?

A. Yes.

15:17:13 To give you an example, when we analyze viruses, if we put them on our real computer, then we would have to wipe that entire computer, which takes some time if they clean the hard drive and you have to reinstall everything.

But if we do that work inside the virtual machine, 15:17:32 then we can run the virus and it will only stay inside of that virtual environment. It won't get out on to our real computer. And the benefit of that is you can keep the work isolated and then you can also shut down your virtual machine and you can start a new one any time you want.

15:17:51 So I can analyze one virus, and then I can just wipe the virtual machine very quickly and start up a new one and I can analyze a second virus very quickly and I can keep all that virus work in the virtual machine. It doesn't have to infect my real machine.

15:18:08 **Q.** Okay.

Could we zoom out? But to the first page, please.

Can you tell from looking at this convenient shot, are we looking at what is -- what is a virtual machine?

A. I can't tell.

15:18:30 **Q.** Okay.

So looking to the right of that -- let's see, the true bar that's in the bottom of the screen. Let's -- if we can zoom in on this tool bar, the whole tool bar. Just up to here. Okay. So we're looking at the tool bar at the bottom

15:18:54 of Exhibit 1446.

And starting on the left is something that appears to be called Penguin Net. Do you know what Penguin Net is?

A. Yes, I do.

Q. What is Penguin Net?

15:19:13 **A.** Penguin Net is a program that allows you to connect securely to remote computers.

Q. Okay.

Does Penguin Net use -- is Penguin Net an SSH client?

A. Yes.

15:19:25 **Q.** What is an SSH client?

A. An SSH client is a program that allows you to encrypt your communications so that it's secure.

Q. So, for example, if you're communicating with a command and control server, could you use a Penguin Net or

15:19:50 another SSH client to make it hard for a new one to see your communications with the command and control server?

A. Yes. So as long as both they -- both of the sender and receiver have the SSH client installed, and can figure correctly, they can communicate with each other securely, 15:20:10 and anybody in between will not be able to see exactly what's happening during that period. And this is behavior I observed over my infected computer.

Q. What did you observe?

A. The encrypted communication via SSH client from going 15:20:34 to the command and control server.

Q. Between a Bayrob Group and the command and control server?

A. Yes.

Q. Were you able to see what was in the SSH 15:20:40 communication?

A. No, I was not.

Q. Because it was encrypted?

A. Yes, because it was encrypted.

Q. All right.

15:20:46 What is that we see to the right of Penguin Net?

A. A program called Total Commander.

Q. And what is Total Commander?

A. It's Total Commander is a file manager. It allows to you see what files are on your computer and to delete them, 15:21:02 move them around, rename them, and very -- very similar to

Explorer, File Explorer in Windows if you're familiar with that.

Q. Okay.

And to the right of that, we see Facebook and that's 15:21:15 up on the screen when we get big. So we'll talk about that in a moment. So skip over Facebook. What do we see to the right of Facebook?

A. So that is a chat program called Pigeon and the person is talking to MasterFraud.

15:21:32 **Q.** Can we zoom out actually? All right.

And can we see up on the screen part of where that chat is occurring?

A. Yes, we can. The chat is occurring here in this window.

15:21:47 **Q.** Now is there any way for you to slide that window over so -- into the chat?

A. No, there's not.

Q. Why not?

A. What?

15:21:56 **Q.** Why not?

A. It's just a picture. I don't have control of this one thing I got.

Q. Just making sure. All right. Does there appear to be Romanian or another foreign language in that chat window?

15:22:12 MR. GOLDBERG: Objection.

MR. O'SHEA: Objection.

THE COURT: Sustained.

Q. Could you please zoom in on that window? All right.

If we could now zoom back out and go to the tool bar
15:22:43 at the bottom. Okay.

So does the green dot represents an ongoing chat with MasterFraud?

A. Yes.

Q. And can you tell what application is being used to
15:23:01 have that chat?

A. The green icon is the same that Pigeon uses.

Q. Okay. So that's Pigeon?

A. Yes.

Q. And did you see this encrypted chat occurring over
15:23:14 your infected system?

A. I did see conversations using Pigeon over my -- my infected box, yes.

Q. You're not sure whether you saw this particular conversation?

15:23:28 **A.** Yeah, I'm not sure.

Q. Okay.

Now, to the right of the MasterFraud tab, do you know what that is that we're seeing?

A. Yes. That's another program that allows you to make
15:23:43 secure connections. It's called Secure CRT.

Q. Can you spell that last, Secure --

A. CRT.

Q. CRT? Okay.

And that would allow you to make secure connections to what? 15:23:57

A. To computers on the Internet that accept secure connections.

Q. Okay.

And then there's one -- looks like there's three icons that are the same there. 15:24:09 One says My Secure something, and the next says VPS Secure, the next says My Secure. Are those all the same program you're referring to?

A. Yes, they are.

Q. What does VPS stand for?

15:24:24 **A.** VPS stands for Virtual Private Server.

Q. What is a Virtual Private Server?

A. It's a server and like we discussed previously, that can be hosted at an online, available 24/7, and generally offered by large companies. And the reason it's called a 15:24:49 Virtual Private Server is because it's not an individual computer. It's multiple -- it's -- you can have a lot of virtual machines on the same hardware, the same computer.

Q. Okay.

And then next to those we see something called Edit 15:25:12 Plus. Do you know what that is?

A. Yeah, Edit Plus is a program for -- for text files, like Notepad, for example, is another one.

Q. For editing text files?

A. Yes.

15:25:23 **Q.** Okay. Okay.

What about next to that? We see, "Socks 3 Win," and it looks like we see actually two of those. The one says Socks 3 Win and the other Socks 3 Wind. You know what those are?

15:25:38 **A.** This is the icon for Internet Explorer, the browser Internet Explorer.

Q. What does the Socks 3 refer to?

A. Socks 3 refers to the title of the page that the person is looking at in Internet Explorer.

15:25:52 **Q.** Okay.

And what do we see next there, AOL Jobs?

A. Yes, AOL Jobs. And the icon and the icon there is a program called Wind SEP, which is also used for transferring files securely from one computer to the other.

15:26:13 **Q.** Okay. And the last one says Yahoo Host, and --

A. I'm not sure. I mean I'm not sure what that signifies.

Q. Okay.

Can you zoom out now? Okay. Now there's a window we see in the background here with some green rows on it. If 15:26:33

you -- would you point to the arrow, use the arrow to point to that. Okay.

A. Yes.

Q. Do you know what that is?

15:26:46 **A.** Yes, I do.

Q. What is that?

A. That is the command and control server and that is a web page that is on the command and control server that allows the Bayrob Group to control all of the infected machines. 15:26:59

Q. Can we look at Page 2 of this exhibit? What's Page 2 of this exhibit?

A. Page 2 is a reconstruction of when they, Bayrob members, connected to their command and control server and accessed the Pay View page on the command and control 15:27:21 server. So what you're seeing here is a page that allows the Bayrob Group to control infected computers.

Q. All right. So how did you get this page?

A. The Bayrob connected to the command and control server via my infected machine. 15:27:42 I was able to capture that traffic and reconstruct this web page.

Q. When you say reconstructed, what do you mean?

A. I mean I took the traffic -- I took the page that was sent over my machine, and I displayed it as it would be seen by the Bayrob Group. 15:28:02

Q. Essentially a screenshot?

A. Yes.

Q. And is this program the same one we see in that window on the previous page?

15:28:13 **A.** Yes.

Q. Okay.

So can you explain how this -- what we're seeing, what this is and how it works?

A. Well, it -- this shows the IP addresses of infected
15:28:34 machines all over the world. And this is how the attackers would be able to see how many infected machines they have and take action for any of those infected machines. And so you can see that they -- on the left-hand side, there's a column called IP. So that's the IP address of all the
15:28:52 infected machines.

And there's a column called City that shows you where the machine is located, and a column called State that shows you where it's located. And then there's information about up time, for example; tells you how long that infected
15:29:14 computer has been turned on and available.

The speed tells you how fast that person's connection is. The version tells you the version of the virus that they have installed on the machine.

And then also there's an action column, and the action
15:29:35 column allows you to take action on the infected machine.

So if you click one of those buttons, an action will occur on the infected machine.

Q. Do you know what those -- what the HP and A, what those different buttons, what action it causes?

15:29:51 **A.** I don't recall at the moment.

Q. Okay.

At the top, it says Stack 166 Online." Do you have an understanding of what that means?

A. Yes. I understand that to mean that there are 166 15:30:06 computers online at the moment available for the Bayrob Group to choose from.

Q. So was this a program they would use, that could be used by the Bayrob Group to proxy from different computers?

MR. O'SHEA: Objection.

15:30:19 THE COURT: Overruled.

THE WITNESS: Yes.

Q. What is the Relay IP address? There's a column several over from the left that says relay. What does that mean?

15:30:33 **A.** So relays are proxies, and they -- the relay column is showing IP addresses and then the password needed to connect to those IP addresses.

Q. It says -- it also says on the upper right, "Relay IP," and it has an IP address after that.

15:30:52 What does that IP represent?

A. That IP address was the IP address of a command and control server, and that was being used by the Bayrob Group.

Q. Is that the relay IP or a relay IP that is currently being used in this screenshot?

15:31:12 **A.** Yes.

Q. All right.

So let's -- so remembering that IP address, 67.205.14.206, let's go back to Page 1 of this exhibit. And if you could zoom in on the upper half of the page.

15:31:40 So looking at the upper half of this page, this is a screenshot. Do you see that same relay IP address somewhere on this page?

A. Yes, I do.

Q. Where do you see that?

15:31:52 **A.** I see it underneath the Facebook.com area, just here.

Q. Okay. And do you see it anywhere else?

A. I also see it over here.

Q. Okay.

So what is that -- what does that row there that we're looking at on the browser, what is that telling us? 15:32:12

A. It's -- this is an add-on that you would need to install to allow you to input the proxy -- proxy addresses and then set that you want to use that proxy.

Q. And what Internet browser are we looking at here? Can we -- you can probably see. 15:32:39

A. Yeah, it says Firefox here.

Q. Does Firefox naturally have a line there for proxy IP address or is this something somebody would have to put on themselves?

15:32:51 **A.** No, Firefox does not are have this. Ordinarily something you have to put on yourself.

Q. So what does the role with IP address 67.205.14.206 tell you about all the Internet activity reflected on this screenshot?

15:33:06 **A.** It tells me that the -- that the web page was requested via a proxy.

Q. Okay.

And does it show that this whole thing is being proxied through that infected computer?

15:33:20 MR. GOLDBERG: Objection.

THE COURT: Overruled. You may answer that.

THE WITNESS: Yes. That appears to be correct.

Q. If we can zoom in now on the, just the Facebook
15:33:33 window. Okay. So looking at just the Facebook window, do you see anything significant there?

A. Yes, I do. I see a -- an advertisement, "Incredible stay-at-home mom makes $7500 each month. We'll tell you how."

15:34:04 **Q.** Is that the same advertisement that we looked at earlier for the money mule?

A. Yes.

Q. Okay.

If we could zoom out. And if we could look at the 15:34:24 tabs of the browser down to here. Yeah. So what are those browser tabs at the top of the screen? You may have to move the arrow a little bit.

A. You're talking about this one?

Q. Yes.

15:34:45 **A.** So that first one, the type -- you see it in the tab at the top, there is the title of the page. And the title of that page is the same title that we see in the advertisements here for the stay-at-home mom advertisement. So that tab is likely showing this page.

15:35:11 **Q.** Okay.

And what do -- what about the next page, the variousopinion.net? Does that show you anything?

A. Yes.

So that page, so the Incredible stay-at-home mom out 15:35:31 here, and this -- this ad is on the website variousopinion.net. And you can see that here. That's -- that's where the -- if you click on this advertisement, you're taken to the website, variousopinion.net, and you'll get information -- the information we saw earlier, the ad we 15:35:50 saw earlier.

And what the next tab up here is showing is there is -- it's showing another page on the variousopinion.net website, and this page is in the slash product folder and the name of the page is click.txt, and that is the -- that 15:36:10 is the page that you showed earlier that shows you how many people have visited variousopinion.net and where they've -- where they've come from.

Q. So does this, what we've looked at, tell you anything about what the user who screenshot this was working on at 15:36:32 the same time of the screenshot?

A. Yes, it does.

Q. What does it suggest to you?

A. It suggests to me that --

MR. O'SHEA: Objection.

15:36:38 THE COURT: Sustained.

Q. Why are the fact that these browser tabs are open significant to you?

A. It's --

MR. O'SHEA: Objection.

15:36:54 THE COURT: Sustained.

Q. The fact that -- is the fact that these browser tabs open significant to you?

MR. O'SHEA: Objection. Withdrawn if it's just a one-word answer, Judge.

15:37:13 THE COURT: Yes. I was going to say. Would you just say yes or no to that, sir.

THE WITNESS: Yes.

BY MR. LEVINE:

Q. Why is it significant to you?

15:37:22 MR. O'SHEA: Objection.

THE COURT: Mr. O'Shea, you want to approach side bar, you may. Otherwise, I'm going to overrule it.

MR. O'SHEA: Fine for now, Judge. No need to --

15:37:34 THE COURT: You don't want to argue? Overruled then.

MR. O'SHEA: Okay.

THE WITNESS: So the reason this is significant is because what this shows me is that the person 15:37:49 who was looking at this Facebook page and who was also using an IP address for a relay, that is the command and control server, also has the advertisement open in another tab and also has the page that tracks how many people have clicked on that ad, opened it in another tab. And to me, it shows 15:38:13 someone is trying to understand how the advertisement is working, are people --

MR. O'SHEA: Objection.

THE WITNESS: -- clicking on this.

THE COURT: Overruled. I'm going to allow 15:38:20 that to stand.

Q. Could you repeat -- could you repeat your answer?

A. It shows that the person who -- whose screen this is, is trying to understand if people are clicking on this advertisement, how successful this advertisement is being.

15:38:35 **Q.** Okay.

MR. O'SHEA: Objection, Judge.

THE COURT: Overruled.

BY MR. LEVINE:

Q. And in general, what does Government's Exhibit 1446 15:38:44 tell you about the way the Bayrob Group operated?

A. I'm sorry. Could you -- could you repeat the question?

Q. Who general -- what does Government's Exhibit 1446, which is what you are looking at, tell you about the way the 15:38:59 Bayrob Group operated?

MR. O'SHEA: Objection.

THE COURT: You understand the question, sir?

THE WITNESS: Yes.

THE COURT: All right. Go ahead.

15:39:04 THE WITNESS: It tells me that they use secure communication programs to communicate both when they are connecting to the computers and chatting to each other. And it tells me that they tested their advertisements and monitored who was clicking on their advertisements. And it 15:39:26 tells me that they connected via a proxy to obscure where they were coming from when they made the connections.

Q. Okay. So let's take this down. Thank you so much.

So the Bayrob Group communicated by encrypted e-mail. We went through that, correct?

15:39:49 **A.** Yes.

MR. O'SHEA: Objection. Form of the question, Judge.

THE COURT: Sustained.

Q. Did we -- did you see --and did we go through Bayrob

15:39:59 Group communicating to each other by encrypted e-mail?

A. Yes.

Q. Did we see and did you go through the Bayrob Group communicating via Yahoo Notepad?

A. Yes.

15:40:11 **Q.** And did you see and go through the Bayrob Group communicating via encrypted Off the Record chat?

A. Yes.

Q. Did you also see evidence of the Bayrob Group communicating through Yahoo Instant Messenger?

15:40:24 **A.** Yes.

Q. All right.

I'd like to show the witness what's been marked as Government's Exhibit 1447. What is Government's Exhibit 1447?

15:40:42 **A.** This is a list of bodies or contacts that were stored in the user who logged into Yahoo Messenger.

Q. Okay. How did you get this?

A. When the -- when members of the Bayrob Group were communicating and they were using my infected machine, when 15:41:03 they logged into Yahoo Messenger, I was able to see the contents of what they saw. So I was able to see their buddy list from when they used my machine.

Q. Were you able to tell what user, which user this was, who logged on?

15:41:20 **A.** Yes, this was Minolta.

Q. Okay. Now, looking at Government's Exhibit 1447, at the time we saw Minolta's Yahoo Messenger buddy list, was one of his buddies MasterFraud?

MR. O'SHEA: Objection. May we approach on 15:41:43 this, Judge?

THE COURT: You may.

(The following proceedings were held at side bar:)

THE COURT: Are you going to finish him today?

MR. LEVINE: I think so.

15:42:07 THE COURT: You think so?

MR. LEVINE: I think so. I have five more pages.

THE COURT: Five more pages? I'm not holding you to it but I'm not optimistic because I have to leave at 15:42:17 4:30.

MR. LEVINE: Okay.

MR. O'SHEA: I'm not sure what he's going to say, but this listed -- sorry.

THE COURT: On or off?

15:42:29 MR. O'SHEA: I'm not sure where this list comes from. I don't think we've set any foundation that's sufficient. I mean these names look like they were typed on some sort of program or Word processor. There's a thing at the top that says 27-Minolta9797 contacts.

15:42:47 MR. LEVINE: I can tell you out of the exhibits -- for all exhibits, we put the file, on almost all, we put the file name at the top. So that was the file name as the exhibit sent to us from --

MR. O'SHEA: Okay.

15:43:00 MR. LEVINE: And that's the witness' name.

MR. O'SHEA: Okay. That's obviously not the format that it came in originally. This is some sort of thing that he created and sent to you with these lists, and it's the same objection that I had and incorporate by 15:43:15 reference that we had, Judge, before relative to the IP addresses. I forget what Exhibit Number that was.

You know, this is not a document in the original native format. This was created by the witness and/or the prosecution and even given a name at the top.

15:43:30 THE COURT: Okay.

But are you objecting to it being shown to the jury? I mean how is it any different than asking him to go up to a blackboard and write out all of this, or is your objection to admissibility?

15:43:49 MR. O'SHEA: It's a little different than the last one, Judge, because the last one was much more information. This has -- one of the biggest, and they keep using the term moniker, you know, and that's going to be their ID fingerprint, you know, so to speak. And that's 15:44:03 gotten -- that's my guy, that's my guy pointing to Radu Miclaus for the record, Judge, right above that. Minolta9797 or 9977.

MR. LEVINE: May I make a suggestion, your Honor? I have to try to resolve this. We have zoomed in. 15:44:21 So you can only see the list here. And for purposes of admitting just the text here, for purposes of admitting the exhibit later, we can redact out this.

THE COURT: But now if we're getting into admissibility, this is a document that he created, correct?

15:44:42 MR. LEVINE: That he found, that he -- he saw on the -- on his infected computer. He saw beyond what he missed.

MR. O'SHEA: Yeah, but this is --

THE COURT: But --

15:44:53 MR. O'SHEA: This is not the list. I'm sorry, Judge.

THE COURT: That's all right.

But this isn't, for lack of a better word, a snapshot of what he found. This is something that he -- that he took 15:45:07 and then he typed up.

MR. LEVINE: I don't think he typed it up. I can ask him that question. I think the answer will be he cut and pasted it from Yahoo. So he -- from Yahoo Messenger.

15:45:20 THE COURT: Okay.

I'm going to allow it to be shown because to me, it's no different than having him get up and make a list on a white board.

But, I'm not going to rule on admissibility now. And 15:45:36 I may very well not allow it in evidence. But, you can certainly always -- I'm going to stop there because I may -- I may allow it, probably not.

MR. O'SHEA: Okay.

MR. LEVINE: We'll cross that bridge when we 15:45:56 come to it.

MR. O'SHEA: Fair enough, Judge. Thank you.

MR. LEVINE: Thank you.

(Proceedings resumed within the hearing of the jury:)

BY MR. LEVINE:

15:46:21 **Q.** Okay.

So can you see this list on your computer?

A. Yes, I can.

Q. And any problems? Okay. So okay. So tell us again what this list represents.

15:46:38 **A.** This represents the contacts for Minolta.

Q. And how did you see it?

A. Myself because Minolta connected to Yahoo Messenger when he was proxying through my infected machine.

Q. Is this a screenshot of his contacts?

15:46:54 **A.** No.

Q. How did you make this document?

A. I took the user names out of the traffic to make it more readable. I copied the user names out of there and put them into a text document.

15:47:10 **Q.** Okay.

Did you do that? Did you type them out or cut and paste them?

A. I cut and paste them.

Q. What is cutting and pasting?

15:47:16 **A.** Copying it exactly as it is from one location to a different location.

Q. Is that when you hit -- it's actually a function on the computer. You hit Control C?

A. Yes, yes. You hit Control C to copy, Control V to paste. 15:47:30

Q. Okay.

So this is the exact list of buddies that you saw Minolta had on Yahoo?

A. Yes.

15:47:38 **Q.** Okay.

And what did you eliminate from this list that we're -- about cutting and pasting?

A. I just made it more readable. It wasn't very readable in the format that I had in the traffic. There's lots of 15:47:56 other data in there. And so I just removed the data that wasn't -- that was distracting from the actual user names.

Q. Okay.

And is one -- one of the buddies of Minolta listed here as MasterFraud1?

15:48:15 **A.** Yes.

Q. And is one of Minolta's buddies listed here as RaduSPR?

A. Yes.

Q. Did you do -- all right. Did you do any research into 15:48:40 these monikers?

A. Yes.

For every moniker here, I searched online to see if I could find any information about who they were.

Q. All right.

15:48:51 And what caused you as to do research into every moniker here?

A. Well, I felt if I could identify -- I already researched the moniker of the Bayrob Group, and I hadn't found a lot of information. I thought if I could identify 15:49:08 some of their friends, some of their contacts in real life, maybe that would help me to understand who the Bayrob Group members were.

Q. Okay.

I want to show now Government's Exhibit 1448, please. 15:49:26 Okay. What is Exhibit 1448?

A. This is a screenshot I took of a Twitter account by the name of RaduSPR.

Q. Okay.

And can you point to where you see RaduSPR here?

15:49:42 **A.** That.

Q. Okay. Do you see it anywhere else on the page?

A. Yes, I see it in multiple locations over here as well, and here, and up here.

Q. Okay. And how did you get -- how did you find this 15:50:02 page?

A. I Googled first.

Q. What do you put into Google?

A. RaduSPR.

Q. RaduSPR?

15:50:11 **A.** Yes. I went to Google, I typed in RaduSPR, and I saw what results I got. I got one result that was on Twitter, and this is the screenshot of the account RaduSPR that I saw on Twitter.

Q. Okay.

15:50:25 And did you find any of these Twitter posts to be significant?

A. Yes, I did.

Q. Why did you find these Twitter posts to be significant?

15:50:34 **A.** The reason I found it to be significant is because they -- the tweets that had been sent here are to an account called White Pool Underscore Net, and White Pool Underscore Net is used as part of Cryptomining. And the dates at which this tweet was sent, sent December 7, 2013, I knew the Bayrob virus was trying to Cryptomine at that time. 15:50:59

Q. Okay.

So being sensitive about the time, but I see we're okay.

So can you explain what whitepool.net has to do with Cryptomining? 15:51:15

A. What whitepool.net is a service that allows you to mine more efficiently. You can send the solutions that you have found to that site and you get, you get the benefit of having a lot of people doing that, and you get a portion of the money that is generated by all the users who are using 15:51:41

White Pool.

Q. All right. So is White Pool a Cryptomining pool?

A. Yes.

Q. Is a Cryptomining pool like a lottery pool?

15:51:59 **A.** No. It's -- it's so if you -- if you were at home and you wanted to mine Cryptomining on your own computer, it may take you a very long time to generate what coin to solve an equation and to get a coin.

So instead, what you can do is send all the results 15:52:22 from the equations you're trying to solve on your computer, you could send them into a pool, and then as long as everyone in the pool agrees to cooperate, and when one person in that pool solves an equation, it doesn't matter if it's you or somebody else, you share the rewards between 15:52:42 everybody who participated in the pool.

Q. And is --

A. I guess in that way, it's like a lottery pool.

Q. Like other office lottery?

A. Yes.

15:52:51 **Q.** Okay.

So is it divided up, though, proportionate to how much processing power you're offering the pool?

A. Yes, you get rewarded in proportion to the amount of work your computer.

15:53:04 **Q.** So, for example, if I have 100,000 computers and you only have one computer, am I going to get basically much, much more of the proceeds than you're going to get?

A. Yes.

Q. Okay.

15:53:16 So with -- those posts are related to Cryptocurrency mining?

A. Yes.

Q. And that was significant to you why?

A. It was significant to me because I knew the Bayrob 15:53:31 virus and my infected machine was being instructed to mine Cryptocurrency and was being instructed to send the -- or participate in White Pool, in the pool that is White Pool. So I knew that was significant.

Q. Your computer was actually being instructed to 15:53:51 participate in this same mining pool?

A. Yes.

Q. Okay.

And can you tell what that's a picture of in the upper left?

15:54:03 **A.** The picture of a person -- the picture of a person.

Q. Yes.

A. It's a picture of a person skydiving.

Q. I want to show you what's been marked as Government's Exhibit 1449. And what is Government's Exhibit 1449?

15:54:25 **A.** It's a screenshot, a picture that I took of a website that I found when I searched for RaduSPR.

Q. How did you get to this website?

A. Again, I went to Google, I searched for RaduSPR, looked at the results, and this is one of the pages that I got in the results. 15:54:42

Q. Okay.

And we may have a translated version. Can we move to the next page and see if it's a translation? Okay. Could we zoom in on the page there? Okay.

15:55:00 And showing where you see RaduSPR on this page.

A. There.

Q. Okay. And what do you see below RaduSPR?

A. I see a person riding a motorcycle. And below that, I see information about the user, that they're a super member, 15:55:25 and that they have 863 posts, that their gender is male, their location is Brasov, and what type of motorcycle they have.

Q. Okay. There's Brasov. And then what is listed there after Brasov?

15:55:41 **A.** Bucharesti and Dava.

Q. Do you know what Bucharesti and Dava?

A. I assume Bucharesti is the city Bucharest. I don't know what Dava is.

Q. Okay. Okay.

15:56:01 Does it list a sport in the post as it's being translated into English at the bottom of the post?

A. Yes, it lists a skydiving.

Q. Okay.

And was there anything significant to you about this
15:56:18 particular post that you found?

A. Yes. There was a lot of significant things. We had seen connections from Brasov in Romania. I had seen connections from my machine from Brasov, Romania. And the name is also what was -- what I found in the contacts, and
15:56:45 also skydiving was listed. And so all of those things together made me think that this was -- that this really was RaduSPR, and that particularly, the connection to Brasov made me suspect this person was involved in the Bayrob Group.

15:57:04 **Q.** What did you -- what do you mean when you saw connections into your infected computer from Brasov?

A. So the -- from time to time, my machine in Romania would be chosen as the first connection in the proxy chain that I talked about. And when that happened, sometimes the
15:57:28 IP addresses that were connected into my machine, the first connection, sometimes those IP addresses were from Brasov.

Q. Okay.

And what is this site that you went to and took a screenshot?

15:57:43 **A.** It's a forum, a discussion forum for a motorcycle, enthusiasm website.

Q. And what was the e-mail address associated with this account as it's listed in the post?

A. RaduSPR@yahoo.com.

15:58:04 **Q.** Okay. I want to move. Let's take this down. I want to move to another topic now.

Do you have any reason to believe that the Bayrob Group was aware that you were investigating them?

A. Yes, I do.

15:58:20 **Q.** What makes you believe that the Bayrob Group was aware that you were investigating them?

A. They left my name in the virus.

Q. They left your name in the virus?

A. Yes, that's correct.

15:58:36 **Q.** Your name, is that Symantec or your personal name?

A. My personal name, Liam.

Q. Can we pull up Government's Exhibit 1450? And can you zoom in on the red area there? Is this the hex header we looked at earlier?

15:59:02 **A.** Yes, it is.

Q. And where do you -- is this the -- is this showing the Bayrob mailer header?

A. Yes, it is.

Q. And what are you highlighting here?

15:59:12 **A.** I'm highlighting where they left my name in the virus.

Q. All right.

And how was your name used in the virus?

A. They created an out of control server name called gayliamasshole.com.

15:59:28 **Q.** Look at Page 2. And can we zoom in? Let's go to Page -- yeah, that's fine. Is that another view of the same?

A. Yes, it is.

Q. Okay.

15:59:48 And if we could go to Page 6 now. Zoom in on the top there as well. And what does that one say?

A. That one says, "Thank you, Liam." The one I've highlighted says thankyouliam.com and the one above that says SymantecversusYahoo.com, and the one above that says 16:00:19 Liamthemule.com, and the one above that says tinycockLiam.com.

Q. I want to ask you questions about the Bayrob Group.

Were you monitoring the Bayrob botnet on September 28, 2016 when the Defendants were arrested?

16:00:52 **A.** Yes, I was.

Q. What happened to the Bayrob botnet after the Defendants here were arrested?

A. I saw no new commands issued to the Bayrob botnet after the arrest.

16:01:01 **Q.** And had you seen any --

THE COURT: Would you state the date again? I thought you said 2019.

MR. LEVINE: No. I'm sorry, your Honor. September 28, 2016.

16:01:10 THE COURT: 2016. Thank you.

MR. LEVINE: Thank you, your Honor.

BY MR. LEVINE:

Q. And tell me again what happened to the Bayrob botnet after the Defendants were arrested?

16:01:19 **A.** I saw no new commands being sent to the infected machines after the arrest.

Q. And have you seen any effort to resurrect the Bayrob botnet since the Defendants' arrest on September 28, 2016?

A. I have not.

16:01:34 MR. LEVINE: No further questions for this witness, your Honor.

THE COURT: Mr. Goldberg, cross-examination?

MR. GOLDBERG: Thank you, your Honor.

CROSS-EXAMINATION OF LIAM OMURCHU

BY MR. GOLDBERG:

Q. Good afternoon, sir.

A. Good afternoon.

16:01:55 **Q.** You first became aware of what you referred -- what you've been referring to as the Bayrob virus in 2007?

A. Yes.

Q. And at some point, you make contact with the FBI regarding what you've learned about it?

16:02:12 **A.** Yes.

Q. And when did you first make contact with the FBI?

A. In 2008.

Q. Okay.

And did you go on exchanging information with the FBI
16:02:23 during the course of your investigation with Bayrob?

A. Not during the entire investigation.

Q. Okay.

So you talked to the FBI at the very beginning and met periodically throughout that period of time?

16:02:40 **A.** I didn't talk to it -- no, not periodically. Yes, I guess periodically.

Q. Periodically?

A. Um-hum.

Q. And who would you check in with?

16:02:49 **A.** With Ryan MacFarlane and Stacy Lough.

Q. Okay.

So you were working in your undercover capacity watching from your machine and checking in with the FBI, correct?

16:03:09 **A.** Correct.

Q. And that was for a number of years, right?

A. Correct.

Q. Okay.

Were you aware whether other antivirus companies were also doing the same type of research? 16:03:22

A. I was aware that other security companies were doing research on Bayrob.

Q. And did you collaborate with them?

A. No, I would say no. We did talk to some other researchers but we didn't collaborate. 16:03:45

Q. You didn't exchange information, correct?

A. No.

Q. Symantec is a big company, right?

A. Yes.

16:03:51 **Q.** Publicly traded?

A. Yes.

Q. Annual sales, about $5 billion?

A. Yes.

Q. Okay.

16:04:00 So your research would be propriety, it would be something you're doing for your company for its benefit, correct?

A. Correct.

Q. Okay.

16:04:10 So for that reason, amongst others, you wouldn't share that information with other private researchers, correct?

A. We do share some information with private researchers.

Q. But you didn't in this case?

A. We did share some information with private researchers. 16:04:28

Q. Did you share -- well, here.

Symantec is Norton Antivirus, right?

A. Yes.

Q. All right.

16:04:35 So -- Kaspersky, that's another antivirus program?

A. Yes.

Q. Did you share information with them?

A. Yes.

Q. Okay. And when did you start doing that?

16:04:43 **A.** We do that on a regular basis.

Q. Regarding what your findings were and what you were monitoring on your infected machine?

A. We share information about viruses with other security companies. And we don't -- we decide at any particular time what specifically we want to share. 16:05:03

Q. Right. Because you want to have better product than your competitors? It's only natural, right?

A. Quite a lot of sharing in the antivirus industry.

Q. But you want to have a better product than your 16:05:17 competitors?

A. We want to have the best product.

Q. So you're not going to tell them exactly what's going on, but you could say hey, there's Bayrob, everybody knows about that, but you're not going to give then the specifics 16:05:30 because you're trying to build a better mouse trap to have more sales than your competitors, correct?

A. We do share information. It's not that we don't share information exclusively to have a better product. We have an agreement in the security industry that we will share 16:05:46 information to benefit the community at large as. So we don't want to have Kaspersky, for example, customers affected very badly because of the fact that we don't share information with them.

So there is a competitive element to it but there is 16:06:07 also an agreement in the industry that we will share information to help each other as well.

Q. Right.

But, what you are working on in your lab in Los Angeles, correct?

16:06:20 **A.** Yes.

Q. That is considered Symantec proprietary information?

A. I'm not sure.

MR. LEVINE: Objection.

THE COURT: Overruled. You understand the question, sir? 16:06:39

THE WITNESS: Not really.

Q. Well, you're developing information on your -- in your lab. You have employees that work with you, right?

A. Yes.

16:06:46 **Q.** You're in charge of the lab?

A. Yes.

Q. You're not the only one doing this work?

A. That's right.

Q. Then the recordings that you've made using Wire Shark, the downloads that you've, for lack of a better word, that 16:07:03 you created, that's -- that's Symantec stuff that's not uploaded to other software providers?

A. It's not a clear cut line. There is information shared. So, for example, files we downloaded, new samples we downloaded of the antivirus, we would share them with all 16:07:22 of our competitors.

Q. Okay. Fair enough.

At the end of the day, there was no way for -- well, what your job was, was to design fixes and other defenses to the Bayrob virus for your customers, right? 16:07:55

A. My job is to protect our customers as best I can.

Q. By doing whatever it is you do with the data that you receive so that you can send them things to your customers that would protect them from the virus?

16:08:13 **A.** That's one of the ways, yes.

Q. But at the end of the day, if you don't know who is actually pushing the buttons on any computer, that could literally be anywhere in the world, correct?

MR. LEVINE: Objection.

16:08:30 THE COURT: Overruled.

THE WITNESS: Sorry. Can you re --

Q. Yes.

At the end of the day, you don't know an actual human being that is responsible. You've told us some information 16:08:40 about getting to somebody that at least had some other moniker, but you don't know, from all the research that you did, who the human beings are?

A. I am -- I didn't see them on the keyboard pressing the buttons, no.

16:08:58 **Q.** Your suspicion was because the first proxy computers were occasionally clustered in Romania, and no other European country, that it was a Romanian-based operation, along with the Romanian language that you found in some of the communications?

16:09:16 **A.** Yes.

Q. Okay.

So since September 28, 2016, has all Romanian hacking, computer fraud ceased?

A. No.

16:09:32 **Q.** So you're still investigating a number of problems, threats, malicious hacking coming out of Romania?

A. We investigate it wherever it comes out. I'm not aware of any investigation specific to Romania at the moment, but I'm sure we're looking at something that's coming out of Romania. 16:09:57

Q. The hacking and malicious software attacks occurred prior to September 28, 2016, and they have occurred after from the state of Romania?

MR. LEVINE: Objection.

16:10:15 THE COURT: Sustained.

Q. Is it -- we looked at -- early on in your testimony, we looked at some code that involved some personal information, not the one we just saw but what you testified yesterday. Is it unusual for any programmer to add personal messages or inside jokes or something like that into a code? 16:11:02

MR. LEVINE: Objection.

THE COURT: Overruled.

Q. Is that something you've seen before?

A. Occasionally.

16:11:10 **Q.** I'm sorry?

A. Occasional -- sorry. I'm not sure what exactly you're referring to, but if I understand, could you -- can you clarify a little bit?

Q. Yeah. This was earlier in your testimony. It was a
16:11:22 long time ago, but I recall you being shown some pictures of the code that was put on your screen and used as an exhibit and there were some words that were interpreted to be Rome?

A. Yes.

Q. Like personal words or jokes or whatever they were?

16:11:49 **A.** Yes.

Q. Is that something that programmers do? Have you seen that before?

A. Occasionally.

Q. But there's nothing unusual about that?

16:11:59 **A.** I would say it's quite unusual.

Q. So you indicated also that you monitor a number of threats, and that some of the -- or many of the European or foreign hacking threats -- I know it originated in China as well -- are made into the United States primarily?

16:12:32 MR. LEVINE: Objection.

THE COURT: Overruled. Can you answer that, sir?

THE WITNESS: I'm sorry. I don't understand the question.

16:12:38 **Q.** Does -- do you find that most or many of the threats originating from outside -- by threats, I mean what we're talking about, computer malware -- originated from outside the United States is infecting in the United States?

A. The majority of it, yes.

16:12:56 **Q.** You know why that is?

A. Because -- one of the reasons is because machines in the US are more valuable. You can make money -- make more money in machines in the US.

Q. I'm going to ask you about Cryptomining for a few 16:13:28 moments.

In theory, it's not illegal, correct?

A. That's correct.

Q. So White Pool was described, I think by Mr. Levine, as something akin to a lottery. Right?

16:13:41 **A.** Yes.

Q. But you know the FBI hasn't shut it down?

A. No.

Q. It's illegal -- it's illegal activity in the United States. It's illegal activity as far as you know?

16:13:51 **A.** Yes.

Q. Okay.

And it works into the whole Cryptocurrency format by having persons do those math equations?

A. Yes. Yes, that's correct.

16:14:03 **Q.** Correct?

A. Yes, that's correct.

Q. And it's not illegal to link computers in order to perform Cryptomining?

A. No.

16:14:11 **Q.** As long as you have permission of the owners to do that?

A. Yes, that's correct.

Q. Okay.

Now you've -- you've testified that with regard to 16:14:20 your machine, the Cryptomining causes a slow down immensely, right?

A. Yes.

Q. At the same time, your machine was being used as a proxy by members of the Bayrob Group to send messages to 16:14:38 each other and to relay from the command and control server, correct?

A. Yes.

Q. So in your experience, isn't it the idea of persons working through a network like this that they want to keep 16:14:58 their presence and their access to the victims' computer a secret?

A. Yes, that's a logic --

Q. Is that operationally beneficial to a malware or a botnet that the person sitting at that computer that's 16:15:23 infected doesn't know it's infected?

A. That is one way that malware operates, yes.

Q. Okay.

So doing something that would intentionally slow it
way down where it couldn't run regular software would be
16:15:39 contrary to the purpose of keeping a secret?

A. Perhaps.

Q. Well, you've testified that was a big clue to you that
your computer was infected, and you had to, in fact,
manipulate it in order to work right?

16:16:03 **A.** Well, I knew my computer was infected without the
computer having slowed down.

Q. To the average person, though, you talked about
400,000 machines over the course of your involvement in
analyzing the Bayrob virus.

16:16:19 The average person out there would be -- either go to
your website trying to locate the Norton virus or going to
Kaspersky trying to download something because they would
know something was wrong with their computer?

A. Yes, that's true.

16:16:39 **Q.** And by doing that, they would be interfering with the
operation of the Bayrob?

A. Yes, I would say that's true.

Q. Okay.

So you had your infected computer up. You remember
16:17:01 the date of that start?

A. I think the first one was around 2010.

Q. And you had multiple?

A. I had multiple, yes.

Q. Were they individual towers or were they virtual
16:17:20 machines or a combination?

A. So the first one was machine under my desk. And there was maybe one or two others like that. And then there was a machine in the data center and two other machines in data centers.

16:17:38 **Q.** And that continued from 2010 continuously to 2016?

A. The amount of computers that I used expanded over time. So 2010, I only had one. By the time it was 2016, I believe I had two.

Q. Did you maintain a permanent record of the data that
16:18:06 you referenced here today and yesterday in your testimony during that period of time?

A. I don't know that I had all -- everything collected. Yeah. I'm not sure.

Q. All right.

16:18:26 Let's -- we'll start with this premise. Your company has unlimited storage potential, correct, pretty much?

A. Probably, yes.

Q. So if you wanted to run a copy of everything that you observed or everything that your computer took in and put
16:18:47 out, connected to the Bayrob virus, you could have done

that?

A. If I had chosen to do so, yes.

Q. Yeah.

And what we have -- you ended up turning over to the 16:19:01 FBI, was it by subpoena, search warrant, combination, neither?

A. Neither.

Q. Okay.

So you just gave them what you thought was relevant to 16:19:15 this investigation at some point?

A. Yes.

Q. Right? You just turned it over, picked what you thought was relevant, and still have everything that you didn't think was relevant?

16:19:25 **A.** I'm not sure exactly what I have. I don't know how complete -- I hope the information I have -- I have information.

Q. Okay.

But we can agree that you -- you sent the stuff that 16:19:41 you thought was relevant to the FBI without a subpoena -- without a subpoena or a warrant, didn't send everything, and you don't know what you have?

A. Yes, I would say that's fair.

Q. Now, Symantec -- when you first discovered this -- the 16:20:09 Bayrob Malware, you started publishing articles in certain computer security, right?

A. Yes.

Q. And that's part of your company's market profile, correct?

16:20:24 **A.** Yes.

Q. Showing that you're doing your job?

A. Yes.

Q. And successfully ferreting out these types of malware and viruses is what you present -- what Symantec presents itself as, being the top of the industry, correct? 16:20:45

A. Yes.

Q. So every time something of this nature would come up, there would be a press release?

A. No, maybe not a press release, but we do -- we -- our policies have changed over the years, but originally, in 16:21:04 2008, we would post something public about the work we were doing on a regular basis.

Q. Okay.

And I'm not going to get too deep into this. So it'll probably be covered by Mr. O'Shea, but when the Defendants 16:21:20 in this case were arrested, Symantec put out a press release, correct?

A. Yes.

Q. Indicating that it had worked with the FBI over a number of years. And now there were some arrests, right? 16:21:33

A. Yes.

Q. And I imagine that the outcome of this trial, if there were a conviction, would also benefit Symantec, correct?

MR. LEVINE: Objection, your Honor.

16:21:51 THE COURT: Sustained.

MR. GOLDBERG: Are you going to put out a press release saying, "Defendants acquitted in the Bayrob scam"?

MR. LEVINE: Objection.

16:21:59 THE COURT: Sustained.

MR. GOLDBERG: May we approach, your Honor?

THE COURT: You may.

(Discussion at side bar off the record.)

THE COURT: Ladies and gentlemen, we've
16:23:27 decided this is a good place to adjourn, good time to adjourn.

Please remember the admonition. Do not form any opinion. Do not talk about the case amongst yourselves or with anyone else. I told you you're going to get sick of me
16:23:39 saying it to you, but I have to always remind you.

Please be downstairs tomorrow morning at 9:00 A.M. We will call for you at that time, bring you up as a group. Make sure you're all are here and healthy tomorrow.

All rise for the jury. Have a good night, folks.

16:23:55 (Proceedings adjourned at 4:23 p.m.)

DIRECT EXAMINATION OF LIAM OMURCHU 336

CROSS-EXAMINATION OF LIAM OMURCHU 537

C E R T I F I C A T E

I certify that the foregoing is a correct transcript from the record of proceedings in the above-entitled matter.

s/Shirle Perkins__________
Shirle M. Perkins, RDR, CRR
U.S. District Court - Room 7-189
801 West Superior Avenue
Cleveland, Ohio 44113
(216) 357-7106